Tellaro SB2

Yubico Yubikey 5C NFC User Guide for macOS

I Prerequisites

- MacOS 13 and above
- Safari 26.0.1
- Yubikey 5C NFC
- Internet connection
- ZIP file issued by an SB2 platform
- USB-C port or USB-C-to-USB-A adapter

II Table of Contents

A1 Installing the Yubico Authenticator Application

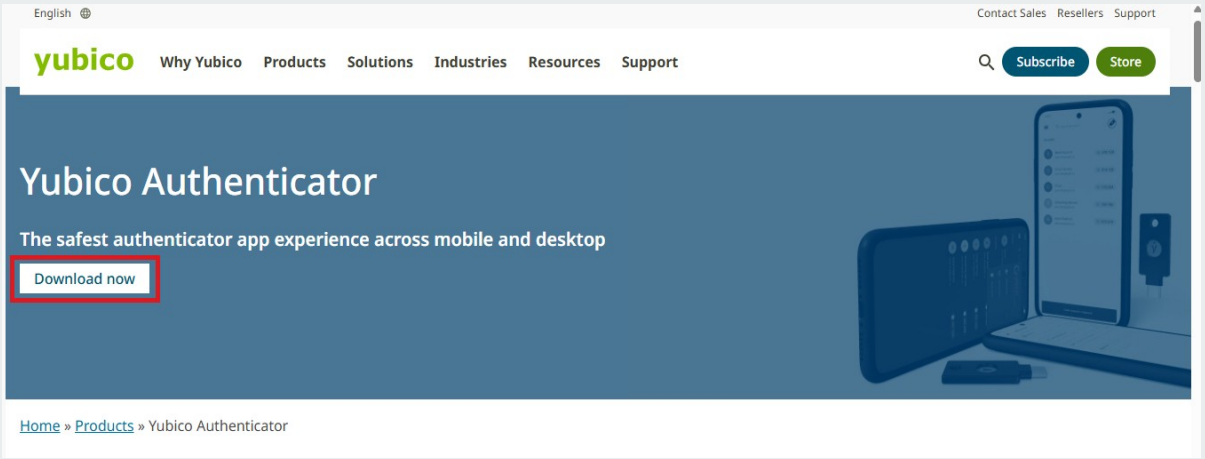
The Yubico Authenticator application is necessary to access and configure the Yubikey 5C NFC Security Key settings and features.

A2 Prerequisites

- macOS 13 or above
- Safari 26.0.1
- Internet connection

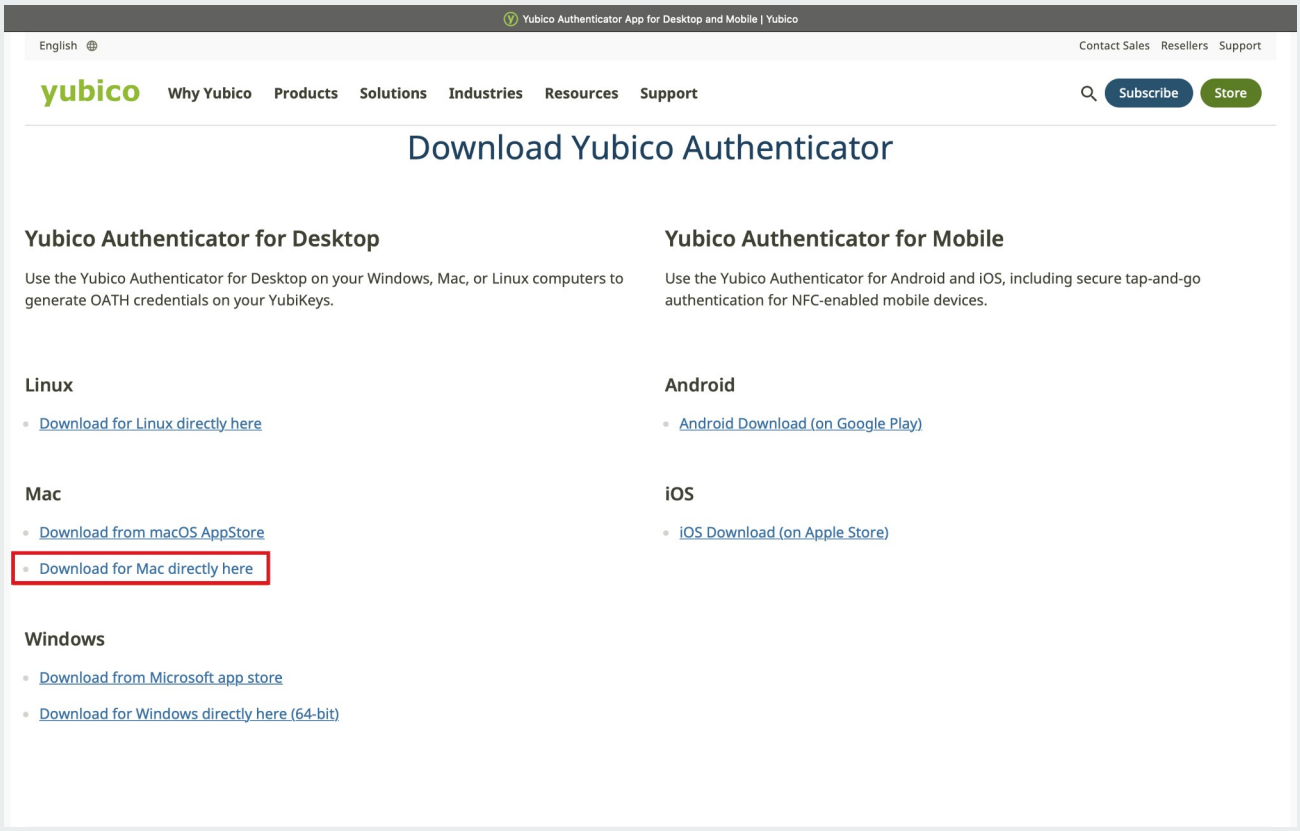
A3 Yubico Authenticator Application Download Page

Navigate to the Yubico Authenticator download page at https://www.yubico.com/products/yubico-authenticator. **Click Download now.**



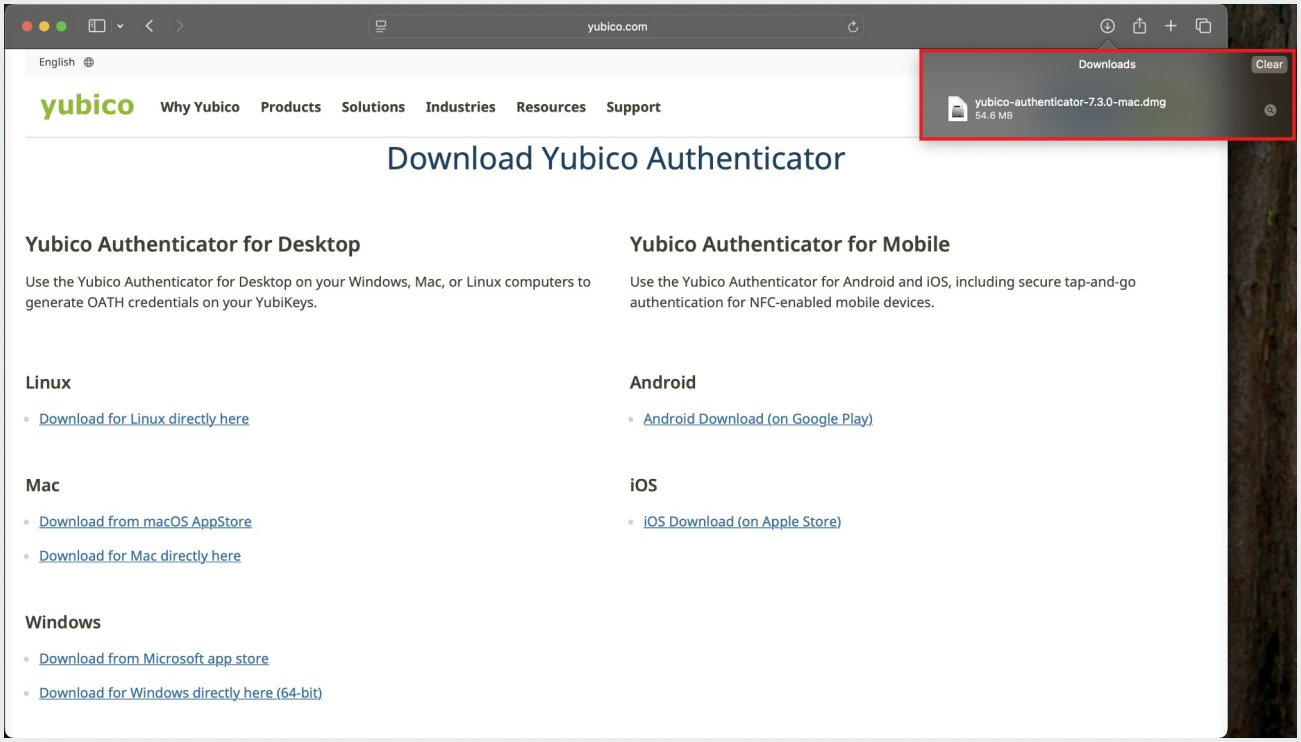
A4 macOS Yubico Authenticator Application

Select **“Download for Mac directly here.” Click it** to start download.



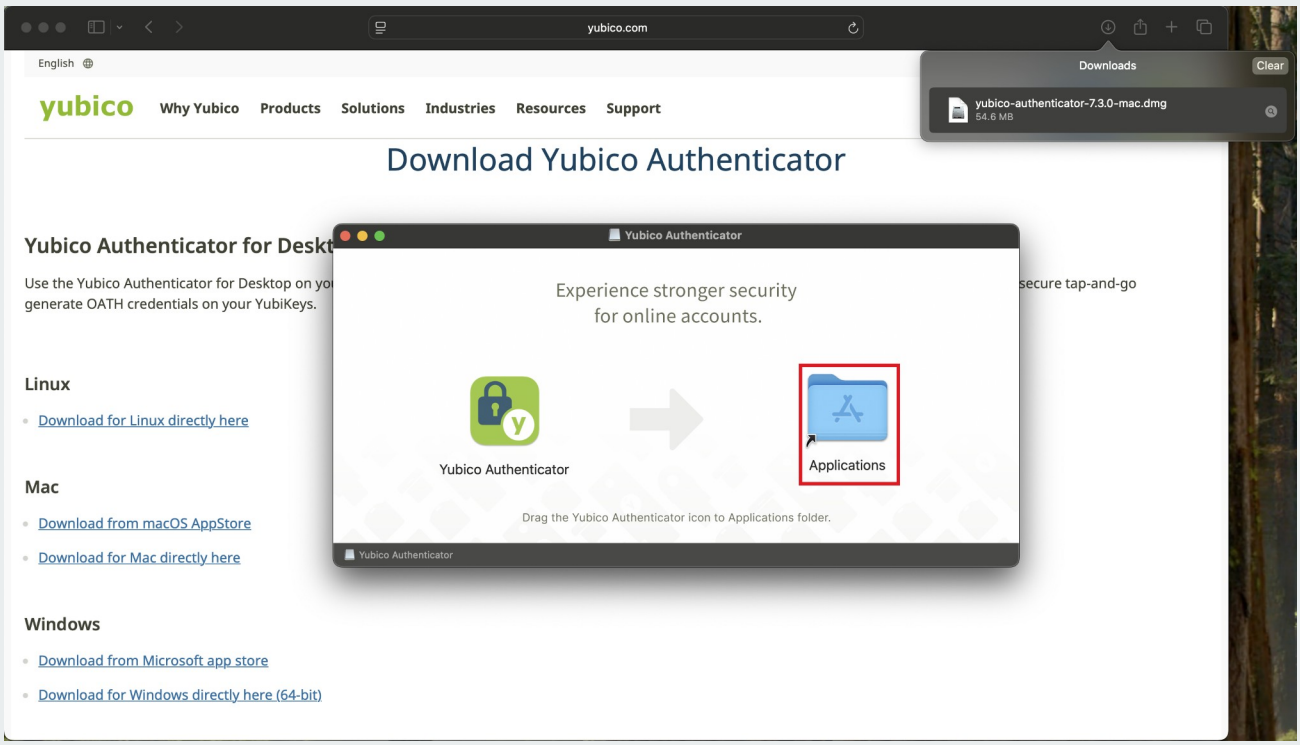
A5 Opening the Yubico Authenticator Application File

After clicking the download link, Safari will display a pop-up confirming the Authenticator application file has been successfully downloaded and ready for installation. **Double-Click the file to open the installer.**



A6 Move the Yubico Authenticator App to the Applications Folder

When the installer window appears, **Drag the Yubico Authenticator icon to the Applications folder.**



A7 Authenticate to Continue Installation

After dragging the **Yubico Authenticator** application to the **Applications folder**, macOS will prompt for **TouchID** or **Mac Account Password** to continue the installation.

The installation of the Yubico Authenticator application is now complete.

SECTION B

B1 Installing an SB2 Root CA Certificate on macOS Keychain Access

When using Security Keys with digital certificates for authentication to an SB2 website, the **SB2 Root CA** certificate is the most critical component in establishing trust with that SB2 site. It verifies that the digital certificate on your Security Key was issued by a trusted Certificate Authority specific to the SB2 website—reflecting the unique "root of trust" established for each SB2 deployment worldwide.

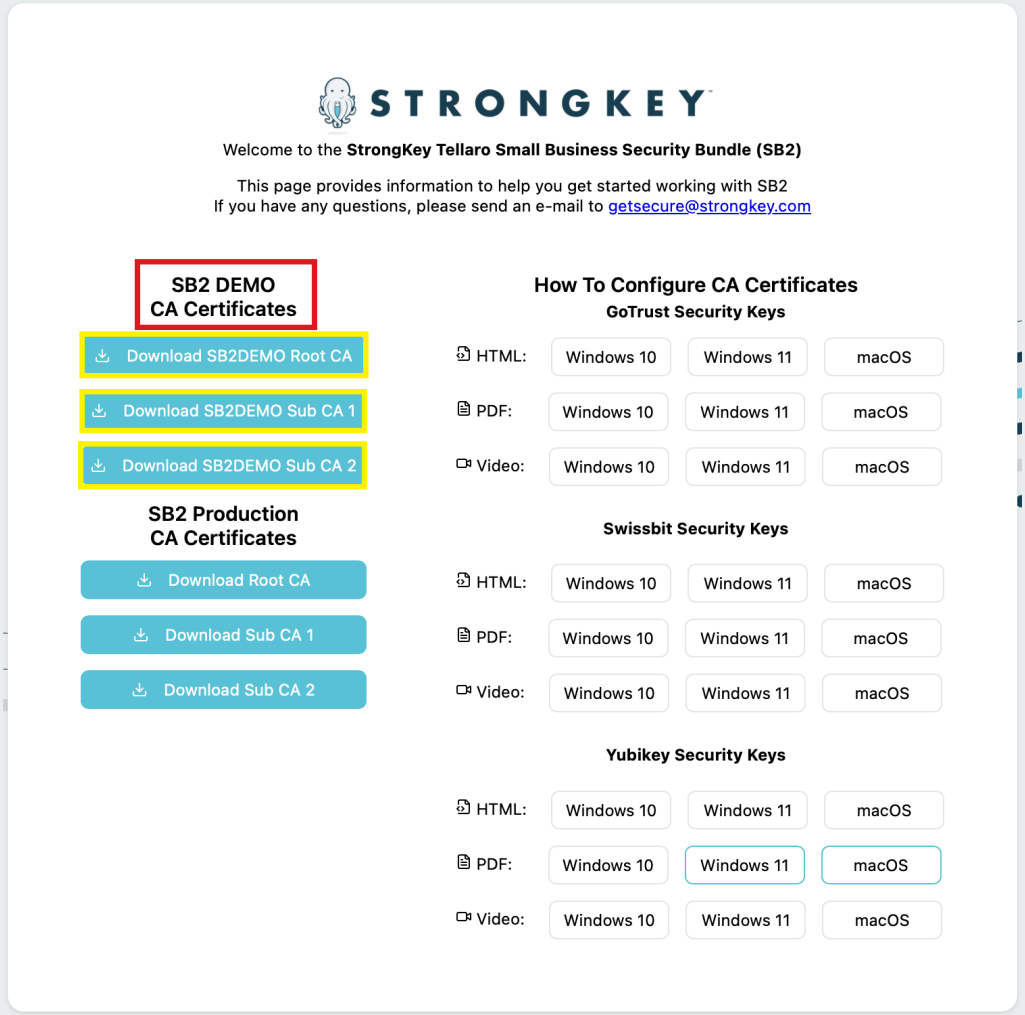
This not only ensures the integrity of the authentication process, but also guarantees that the trust established between the Security Key you were given and the SB2 site, is unique from every other SB2 site in the world. This ensures attackers cannot scale an attack on any other SB2 website even if they managed to compromise one through an insider attack.

B2 Prerequisites

- macOS Sequoia 15.7.1
- ZIP File issued by the Administrator of an SB2 platform at your site; or
- Individual CA certificate files issued by the Administrator of an SB2 platform at your site.
- NOTE: In the event the SB2 Administrator provided individual files for the **SB2 Root CA** and **SB2 Subordinate** CA certificates, you may import them directly from the stored location on your computer without the need for the ZIP file – the process is similar, starting from step B10.

B3 Access the SB2 Demo MPKI Portal

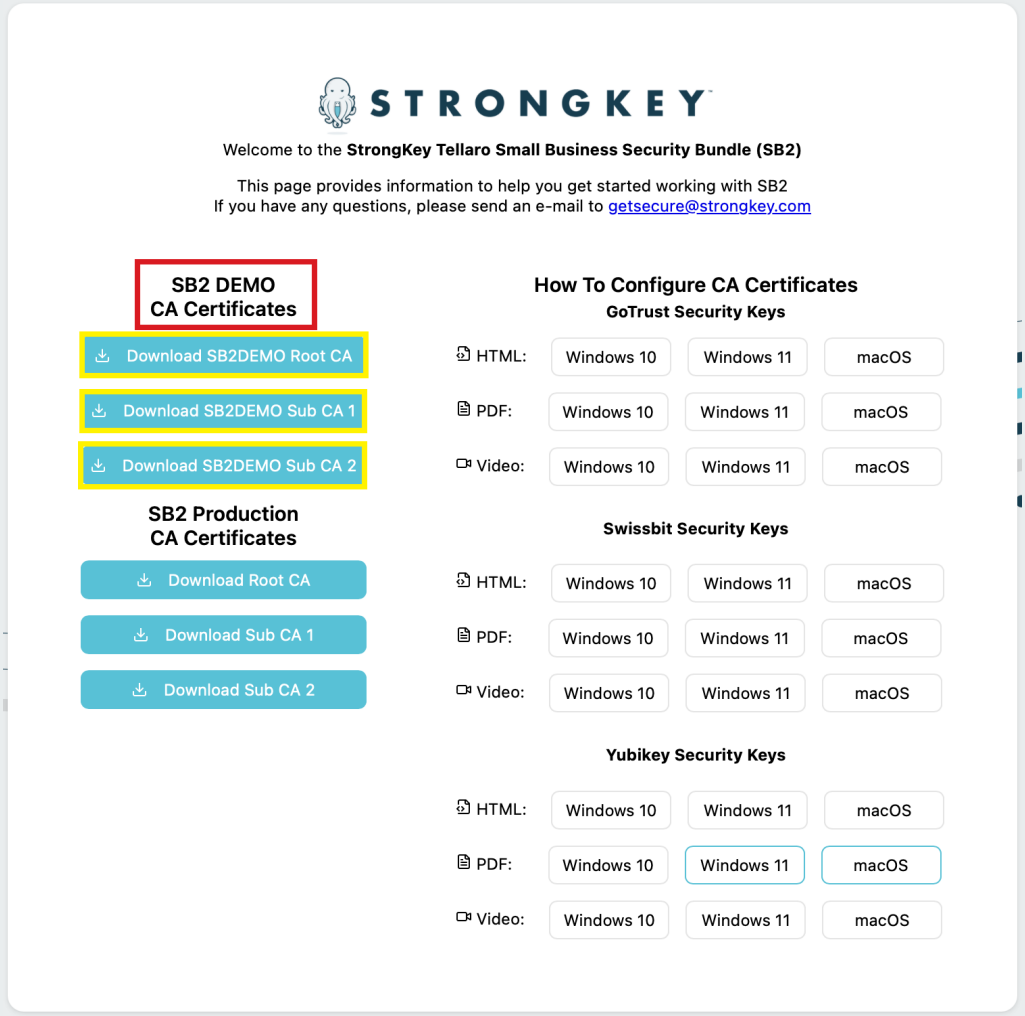
All required CA certificates are available for download for the StrongKey Tellaro Small Business Security Bundle© (SB2) at https://demo.strongkey.com/mpki/index.html. Comprehensive SB2 documentation is also accessible through this site. While this section focuses on installing the Root CA, please note the subordinate CAs are also available for download and installation.



B4 SB2 DEMO CA Certificates

At the MPKI portal, locate the available CA Certificate download options (yellow boxes) and download the three files (Section C documents installing the remaining Subordinate CAs). Each of the following certificate files are required:

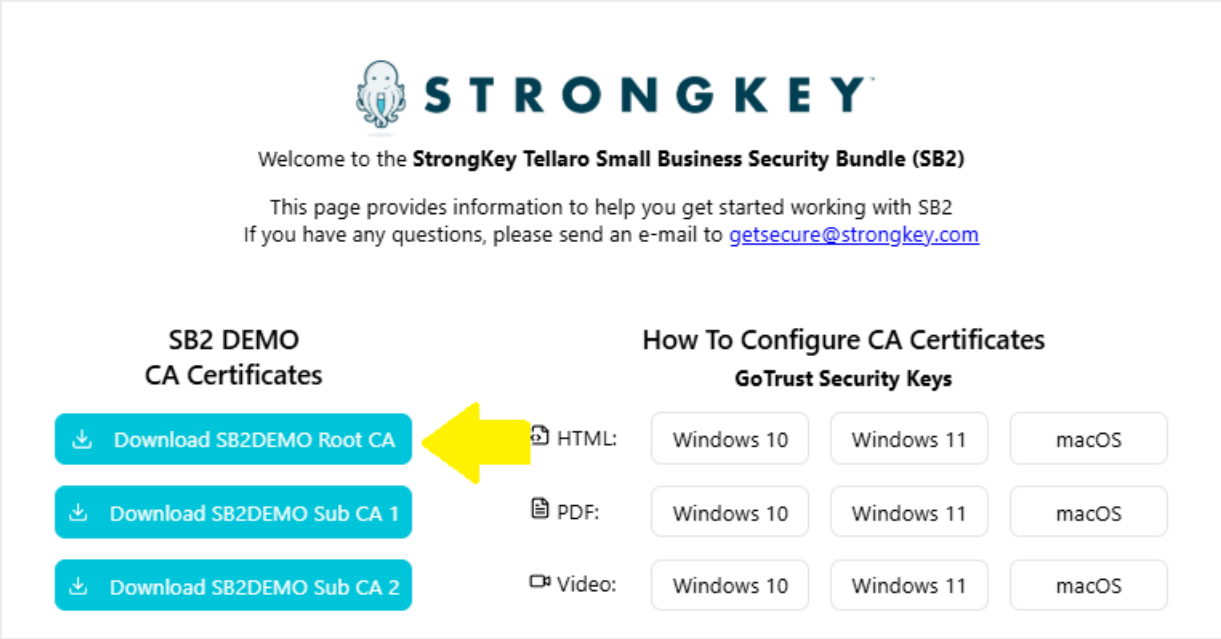
- SB2DEMO Root CA
- SB2DEMO Sub CA1
- SB2DEMO Sub CA2



B5 Download SB2 DEMO Root CA

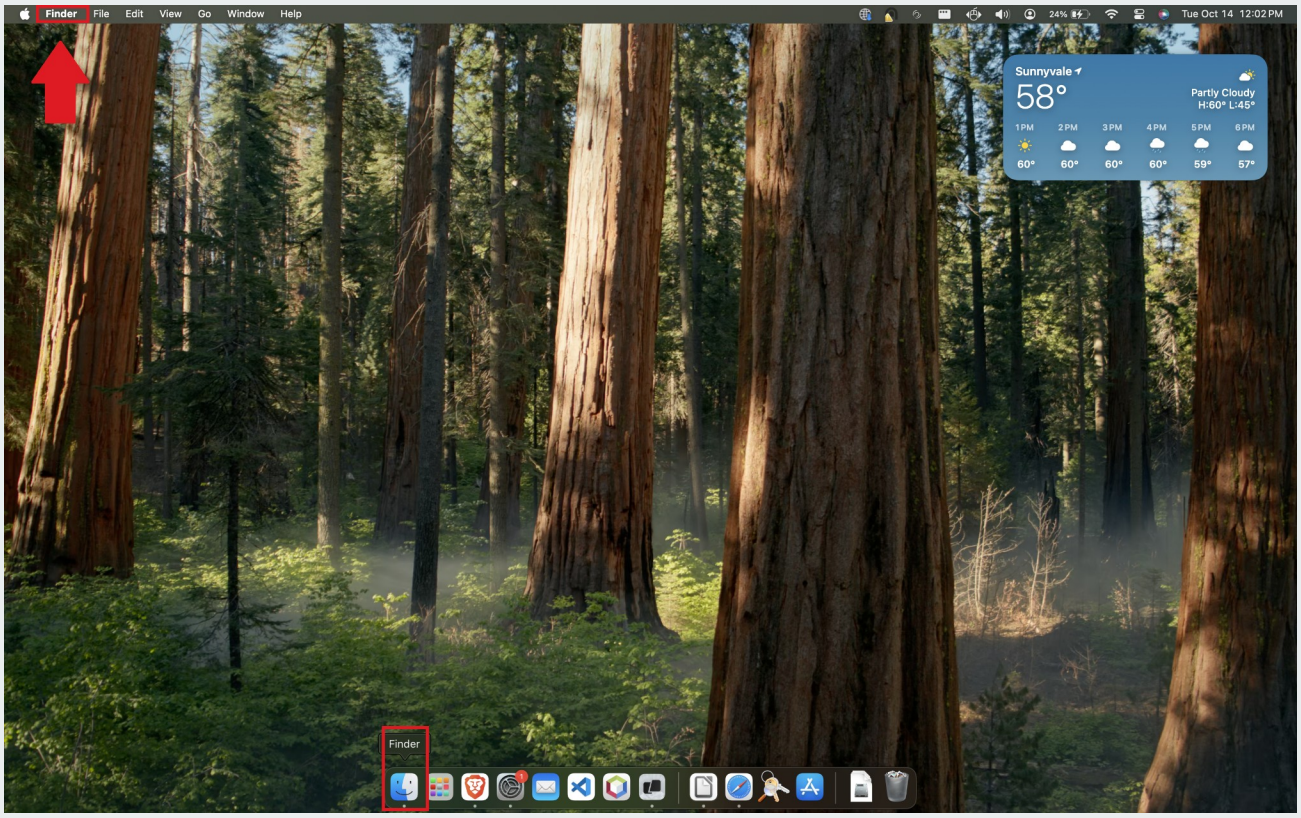
To download the Root CA, simply select the SB2DEMO Root CA button. After clicking the download link, Safari will display a pop-up confirming the file has been successfully downloaded.

Repeat this process for the **SB2DEMO Sub CA1** and the **SB2DEMO Sub CA2** files.



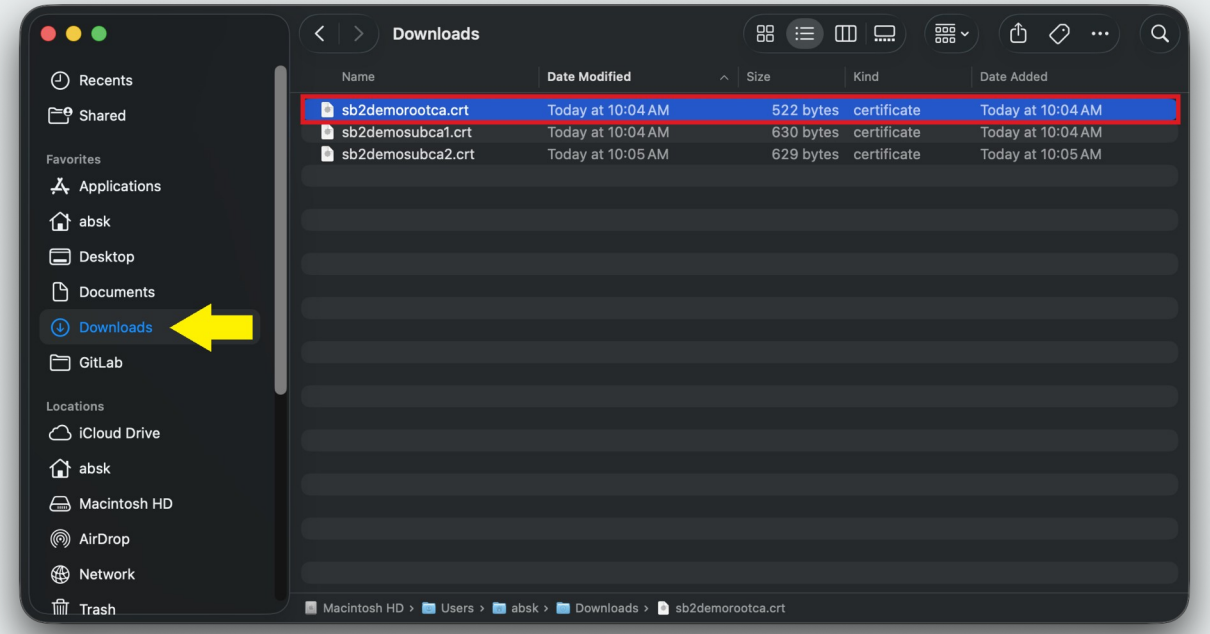
B6 Access macOS Finder

To get started installing the certificates, open the **Finder** application by clicking its icon in the **Dock** or by selecting it from the menu in the upper left corner of your screen.



B7 Locate Downloaded SB2 Root CA File

Navigate to the **Downloads** folder in **Finder**. Locate the **SB2 Root CA file** and **right-click** it. *Please note* that your specific **SB2 certificates file** may have a different name. Ensure you know the correct file name before proceeding.



B8 Open Keychain Access

Launch **Keychain Access** by searching with **Spotlight** [⌘ + Space] (refer to Image 1), or by navigating to **Applications** in **Finder** (see Image 2).

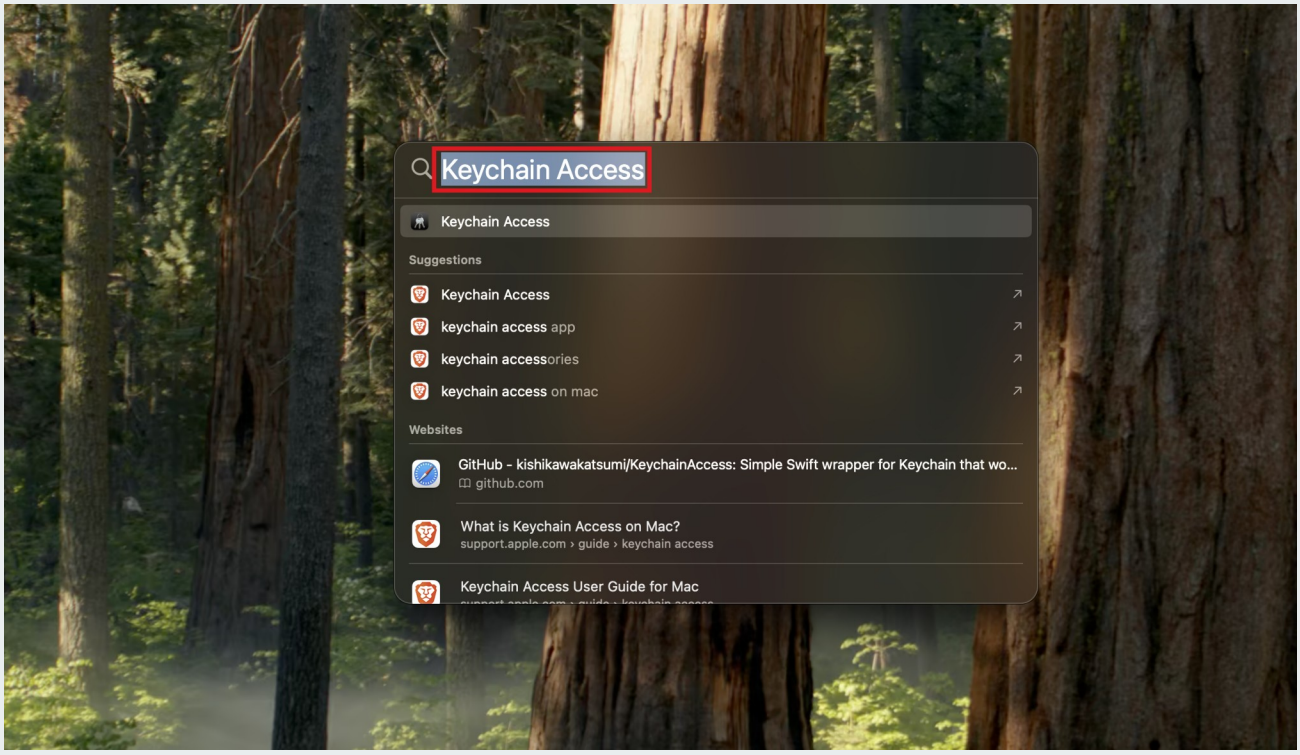


Image 1

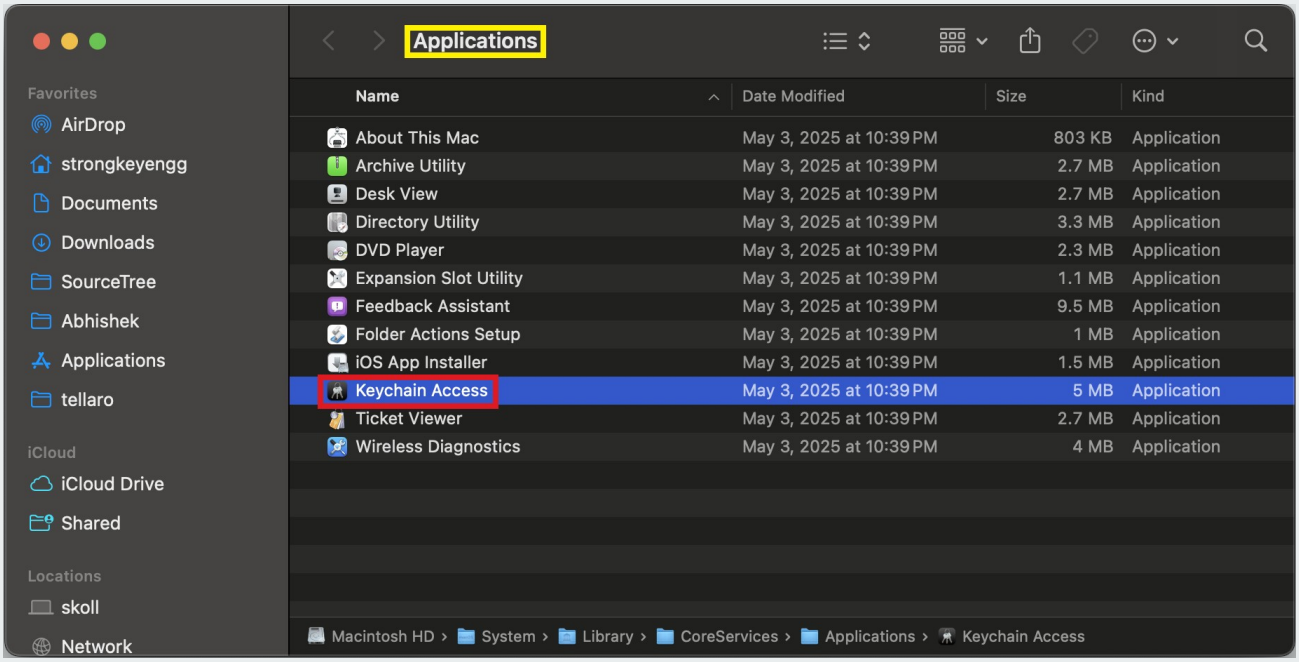
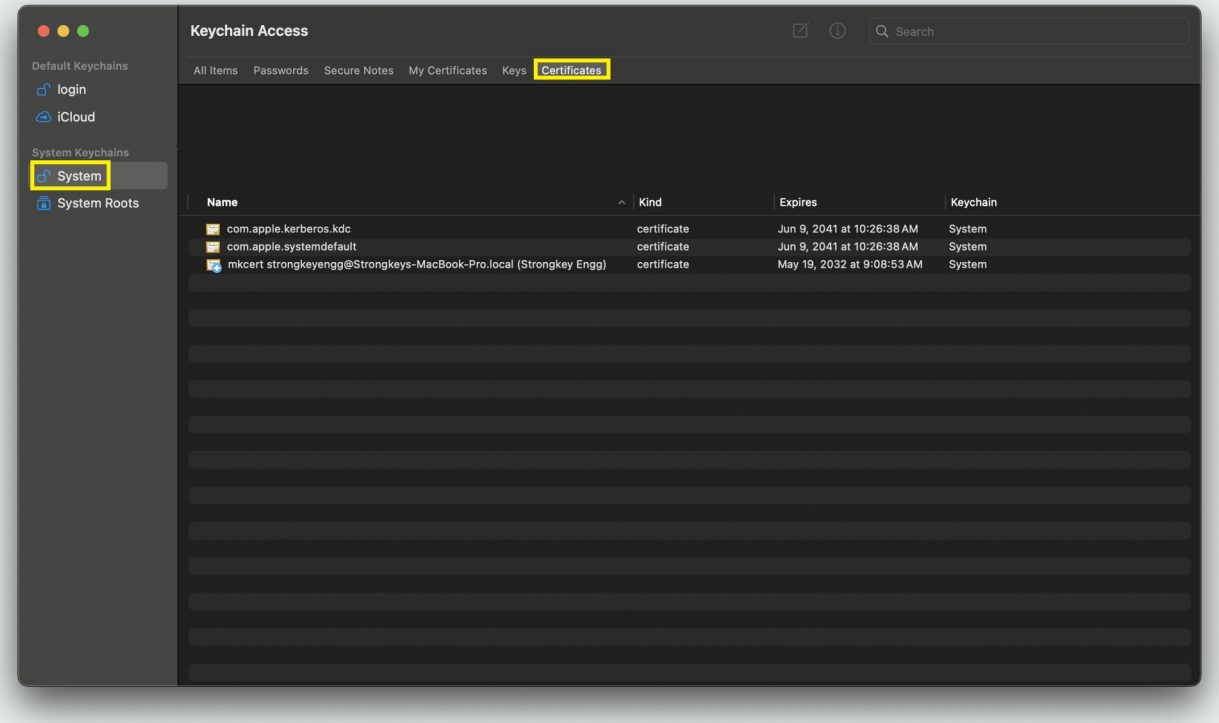

Applications
Favorites
AirDrop
strongkeyengg
Documents
Downloads
SourceTree
Abhishek
Applications
tellaro
iCloud
iCloud Drive
Shared
Locations
skoll
Network
Name
Date Modified
Size
Kind
About This Mac May 3, 2025 at 10:39 PM 803 KB Application
Archive Utility May 3, 2025 at 10:39 PM 2.7 MB Application
Desk View May 3, 2025 at 10:39 PM 2.7 MB Application
Directory Utility May 3, 2025 at 10:39 PM 3.3 MB Application
DVD Player May 3, 2025 at 10:39 PM 2.3 MB Application
Expansion Slot Utility May 3, 2025 at 10:39 PM 1.1 MB Application
Feedback Assistant May 3, 2025 at 10:39 PM 9.5 MB Application
Folder Actions Setup May 3, 2025 at 10:39 PM 1 MB Application
iOS App Installer May 3, 2025 at 10:39 PM 1.5 MB Application
Keychain Access May 3, 2025 at 10:39 PM 5 MB Application
Ticket Viewer May 3, 2025 at 10:39 PM 2.7 MB Application
Wireless Diagnostics May 3, 2025 at 10:39 PM 4 MB Application
Macintosh HD › System › Library › CoreServices › Applications › Keychain Access

Image 2

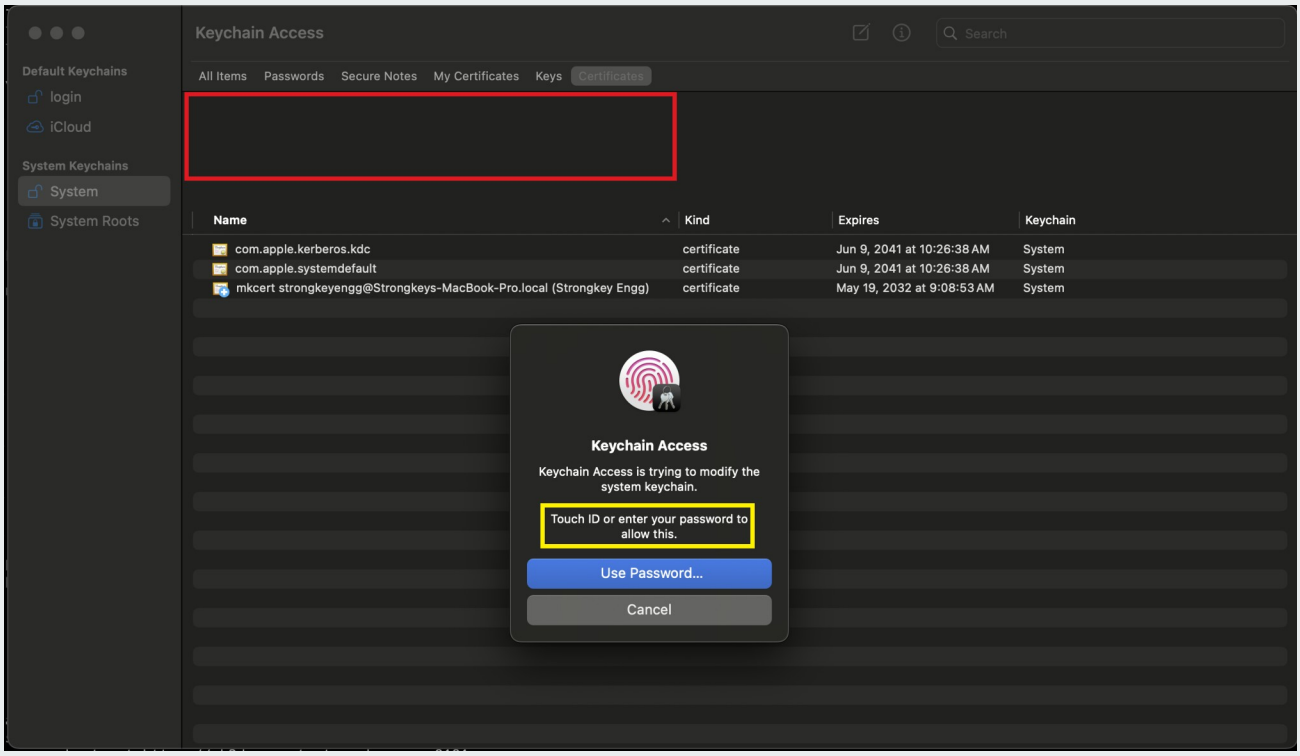
B9 Navigating in the KeyChain Access Application

After launching the **KeyChain Access** application, the following screen appears. Select **System** in the sidebar, followed by **Certificates** in the top menu.



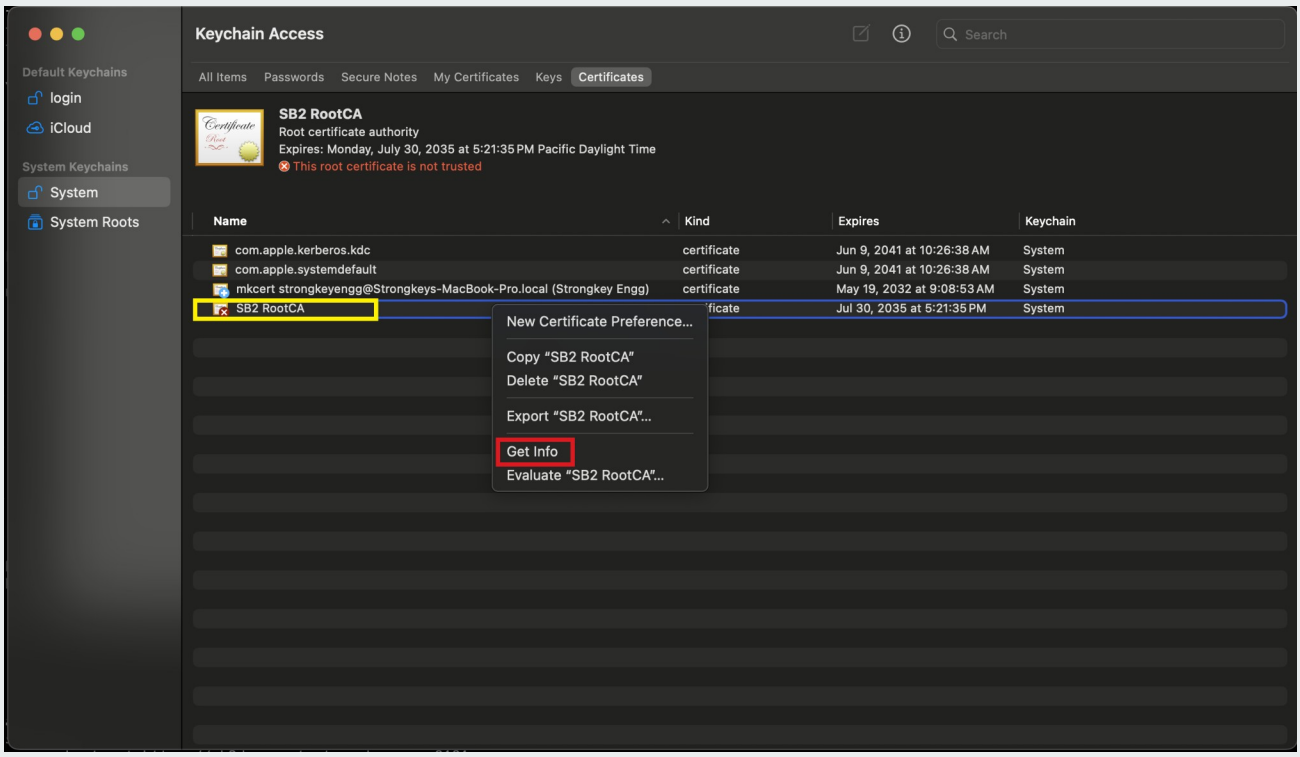
B10 Importing Certificates

Next, drag the **SB2-RootCA.crt file** into the **Keychain Access** window to begin the certificate import process. The macOS will prompt you to authenticate using Touch ID or an account password to complete the import.



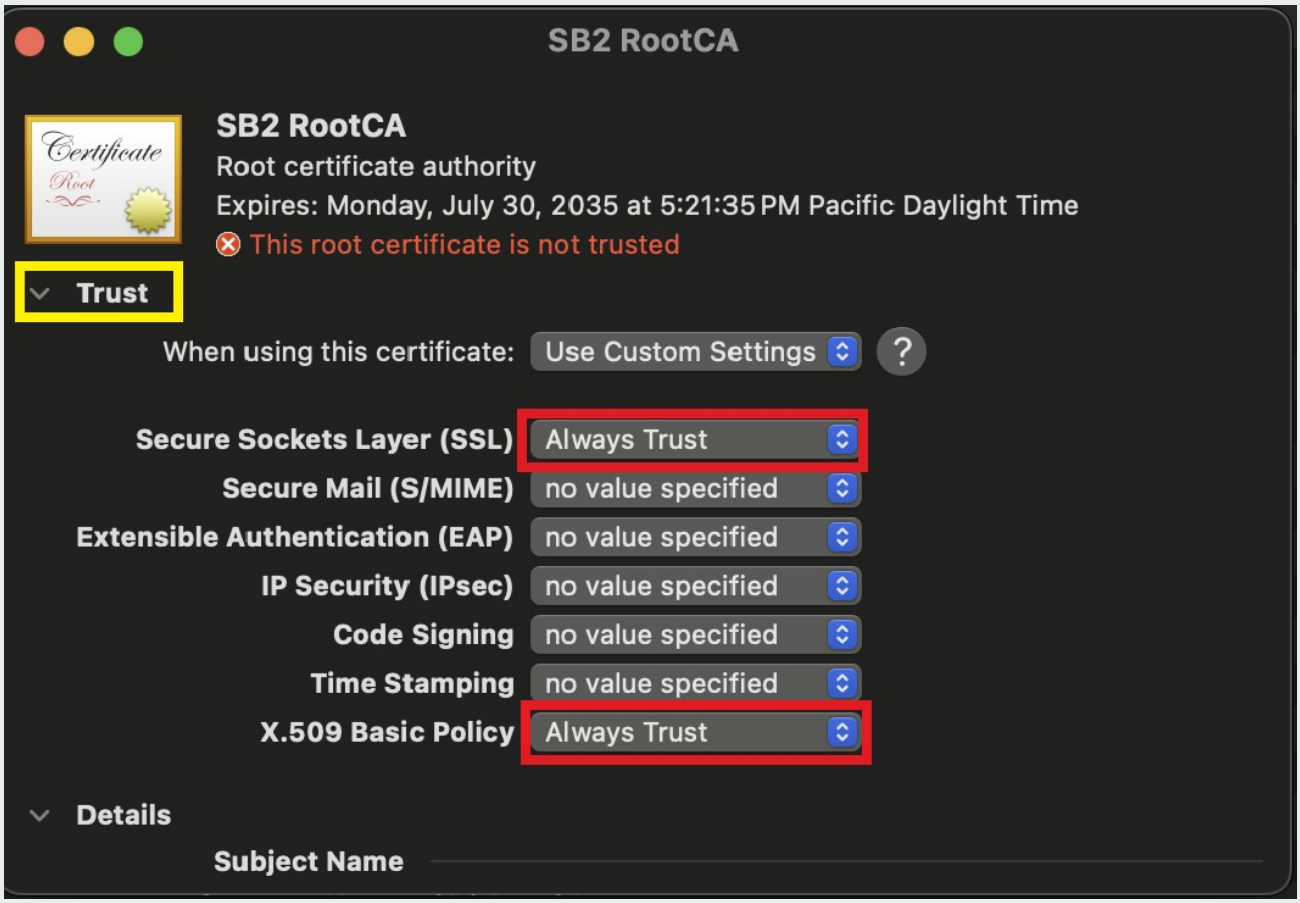
B11 Access the SB2 RootCA Certificate Details

Right-click on the imported **SB2 RootCA** certificate, then select **Get Info** to view its details.



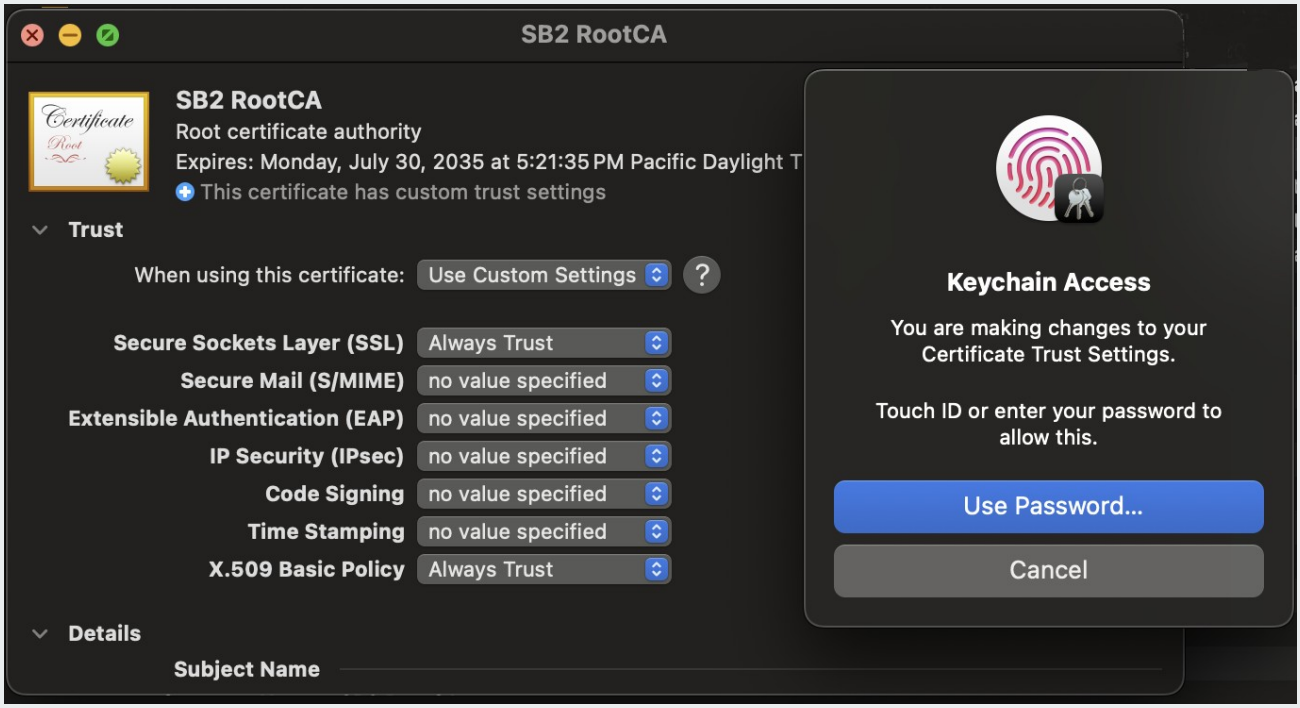
B12 Trust the SB2 RootCA Certificate

To view the **Trust** details, click the down arrow next to the Trust option. Then, select **Always Trust** for both **Secure Sockets Layer** (SSL) and **X.509 Basic Policy**.



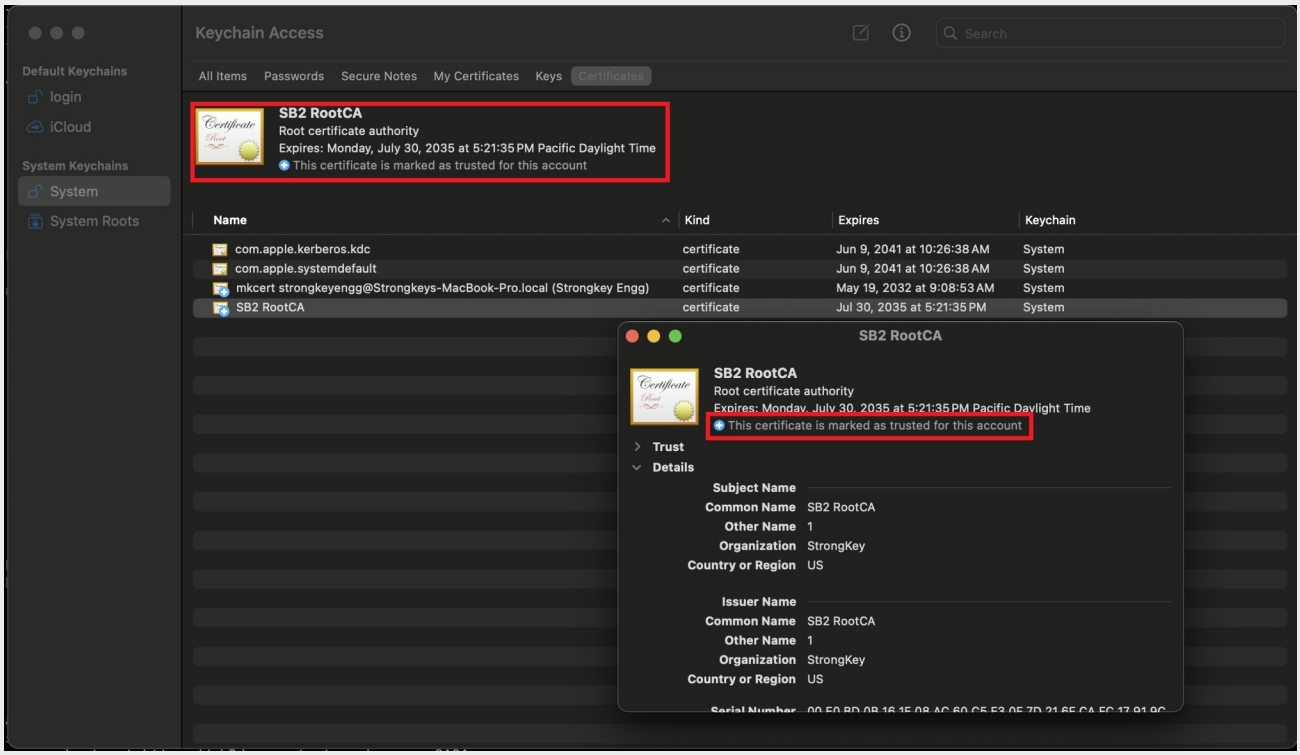
B13 Authenticating the Changes to the SB2 RootCA Certificate

After the SB2 RootCA **Get Info** window is closed, macOS prompts for authentication, using either **Touch ID** or the **macOS account password**, to confirm changes to the Trust settings.



B14 Confirming the Trust Changes

Click **Next** to continue. To confirm the trust settings, **right-click** the SB2 RootCA certificate and select **Get Info**. A successful import and **trust** is indicated by the message: ***"This certificate is marked as trusted for this account."***



SECTION C

C1 Importing an SB2 Subordinate Root CA Certificate into macOS Keychain Access

Subordinate CA certificates play a vital role within the SB2 platform. They are part of the “certificate chain” establishing trust between the digital certificate on your Security Key and the SB2 Root CA embedded within the SB2 platform.

C2 Prerequisites

- macOS Sequoia 15.7.1
- ZIP File issued by the Administrator of an SB2 platform* at your site; or
- Individual CA certificate files issued by the Administrator of an SB2 platform at your site
- NOTE: In the event the SB2 Administrator provided individual files for the **SB2 Root CA** and **SB2 Subordinate** CA certificates, you may import them directly from the stored location on your computer without the need for the ZIP file – the process is similar, starting from step D5

C3 Accessing Downloaded Subordinate Root Certificate Files

To get started, launch **Keychain Access** by searching with **Spotlight** [⌘ + Space] (refer to Image 1), or by navigating to **Applications** in **Finder** (see Image 2).

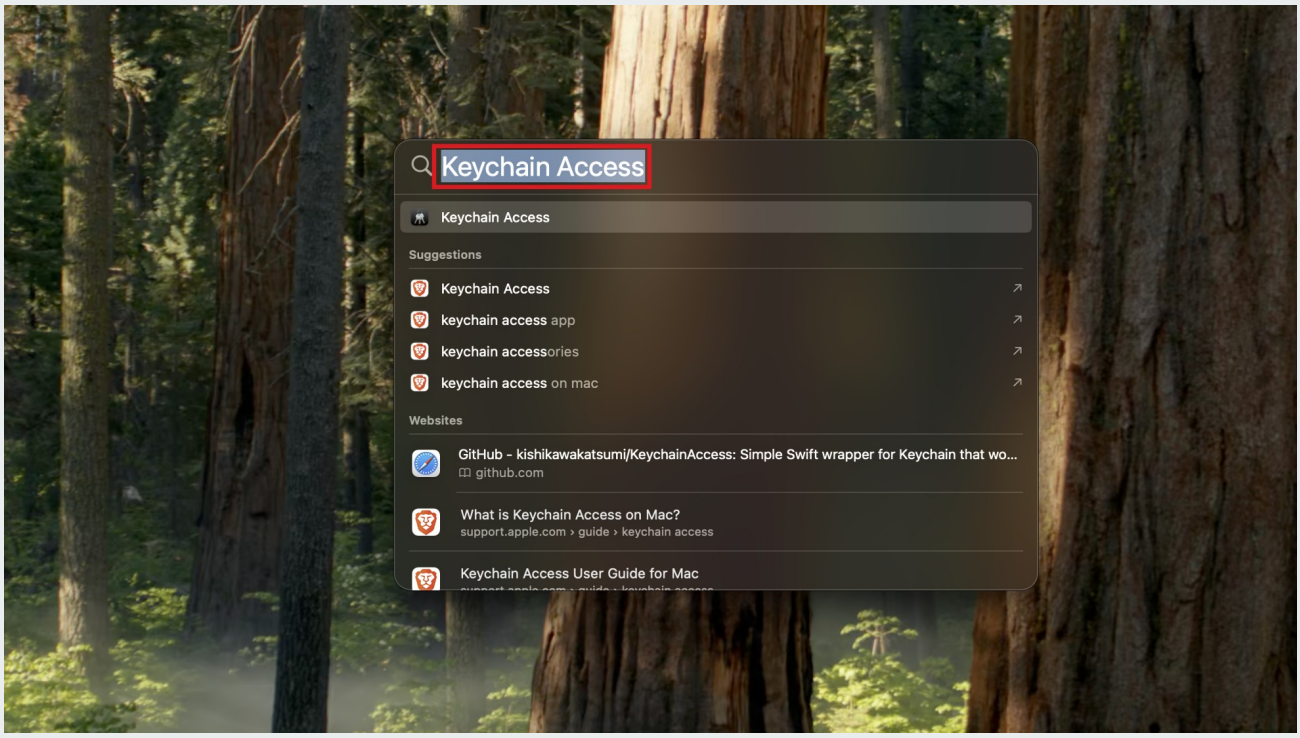


Image 1

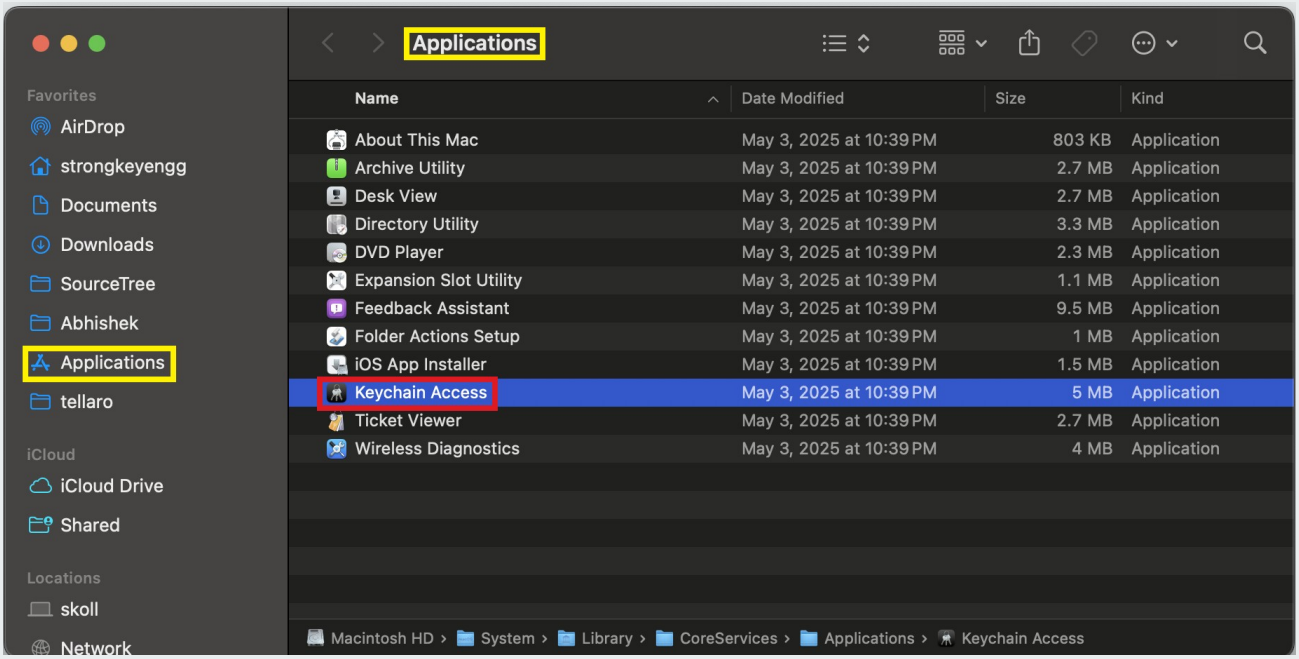
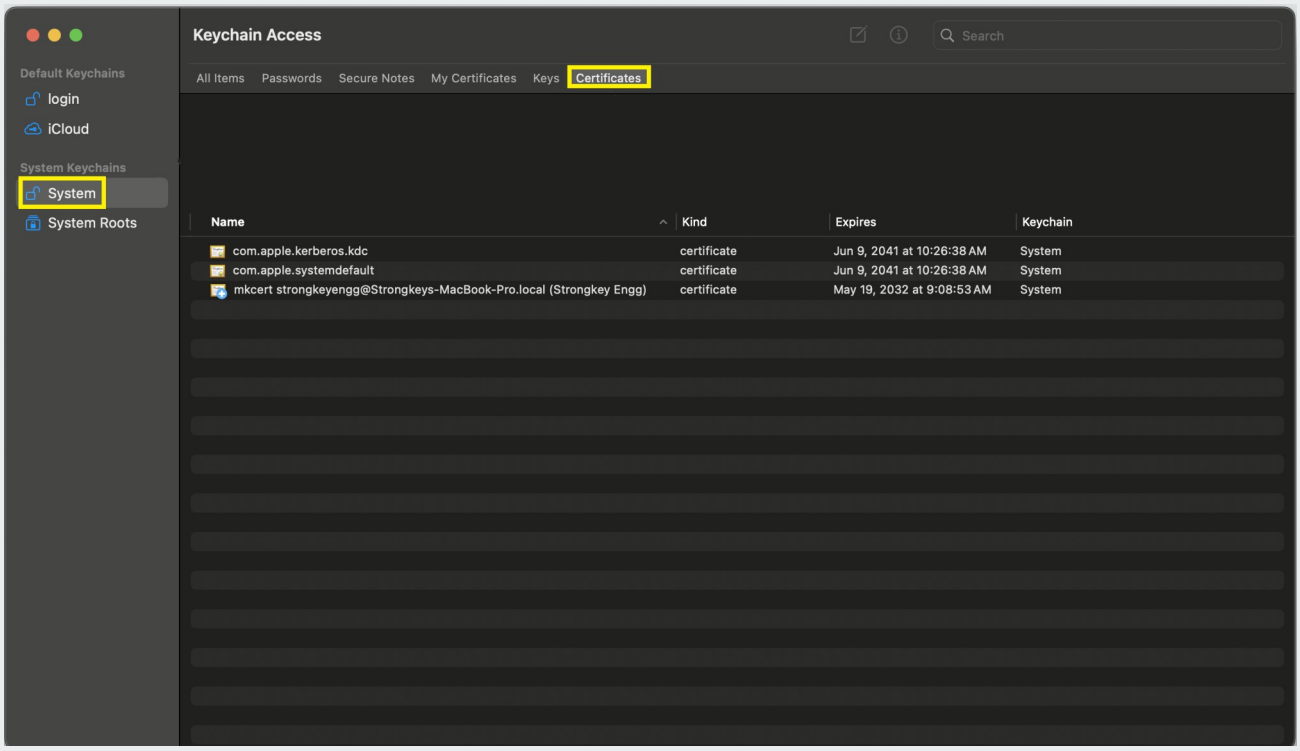

Applications
Favorites
AirDrop
strongkeyengg
Documents
Downloads
SourceTree
Abhishek
Applications
tellaro
iCloud
iCloud Drive
Shared
Locations
skoll
Network
Name
Date Modified
Size
Kind
About This Mac May 3, 2025 at 10:39 PM 803 KB Application
Archive Utility May 3, 2025 at 10:39 PM 2.7 MB Application
Desk View May 3, 2025 at 10:39 PM 2.7 MB Application
Directory Utility May 3, 2025 at 10:39 PM 3.3 MB Application
DVD Player May 3, 2025 at 10:39 PM 2.3 MB Application
Expansion Slot Utility May 3, 2025 at 10:39 PM 1.1 MB Application
Feedback Assistant May 3, 2025 at 10:39 PM 9.5 MB Application
Folder Actions Setup May 3, 2025 at 10:39 PM 1 MB Application
iOS App Installer May 3, 2025 at 10:39 PM 1.5 MB Application
Keychain Access May 3, 2025 at 10:39 PM 5 MB Application
Ticket Viewer May 3, 2025 at 10:39 PM 2.7 MB Application
Wireless Diagnostics May 3, 2025 at 10:39 PM 4 MB Application
Macintosh HD › System › Library › CoreServices › Applications › Keychain Access

Image 2

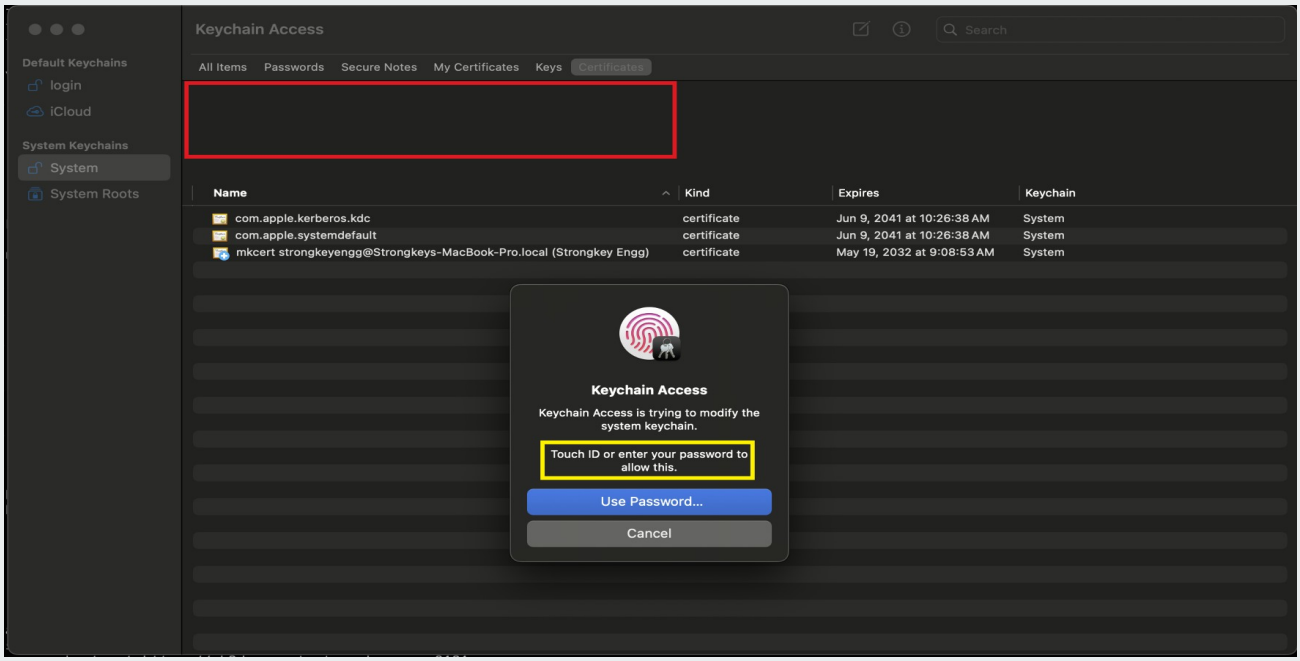
C4 Navigating in the KeyChain Access Application

After launching the **KeyChain Access** application, the following screen appears. Select **System** in the sidebar, followed by **Certificates** in the top menu.



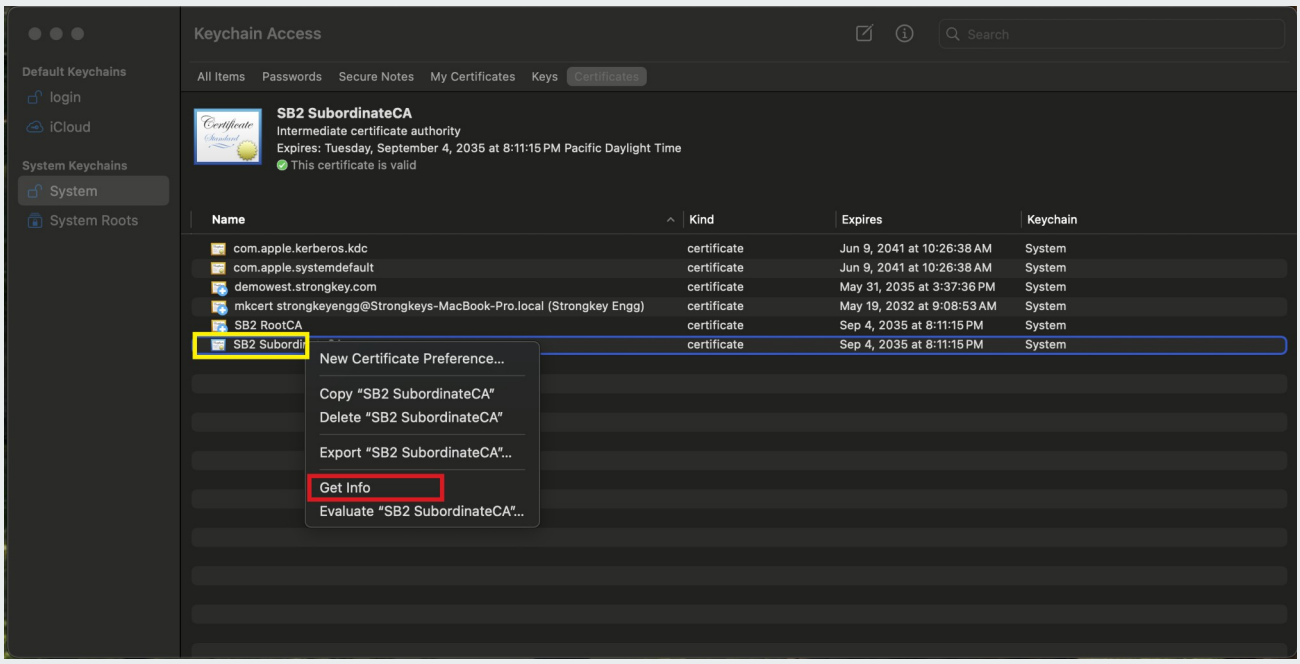
C5 Importing Certificates

Next, drag the **SB2-SubordinateCA.crt file** into the **Keychain Access** window to begin the certificate import process. The macOS will prompt you to authenticate using Touch ID or an account password to complete the import.



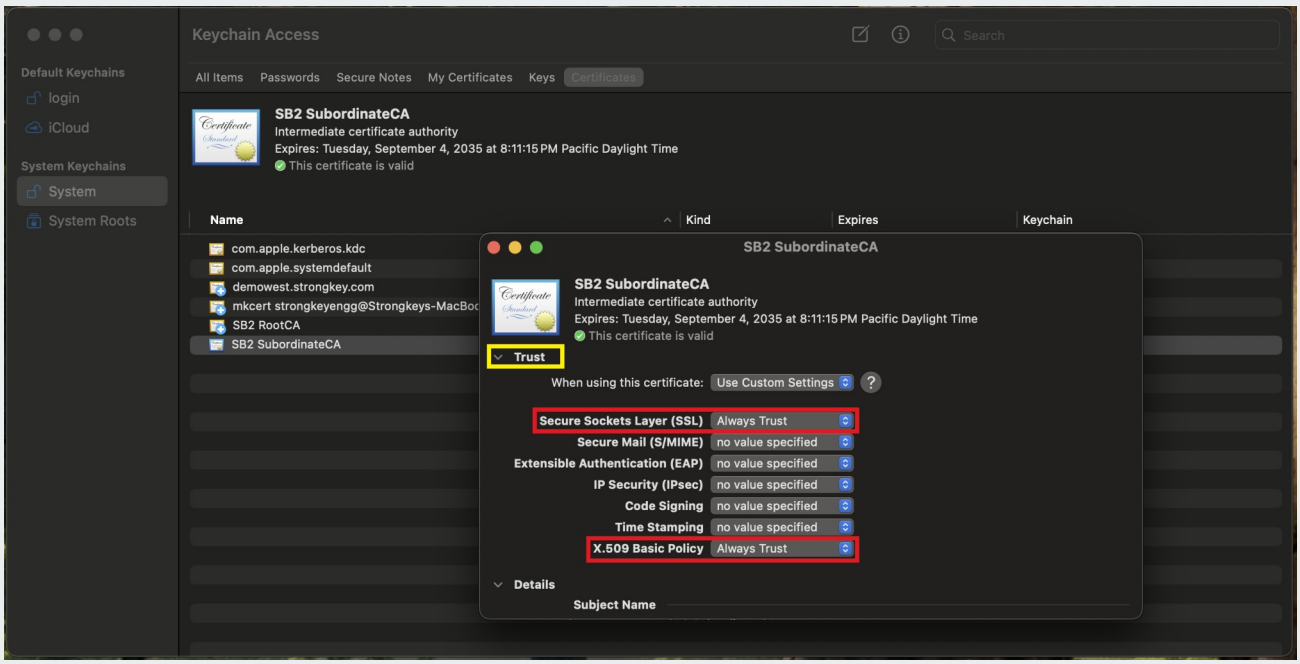
C6 Access the SB2 SubordinateCA Certificate Details

Right-click on the imported **SB2 SubordinateCA** certificate, then select **Get Info** to view its details.



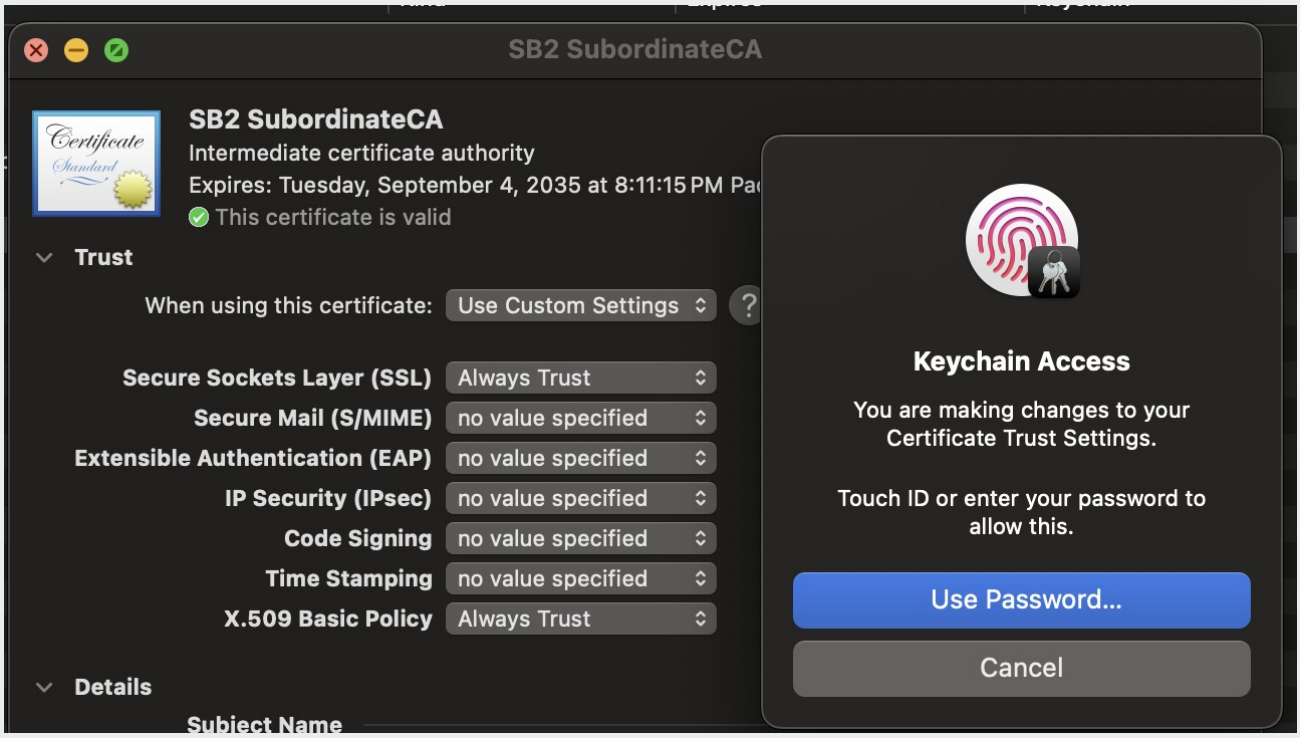
C7 Trust the SB2 SubordinateCA Certificate

To view the **Trust details**, click the **down arrow** next to the **Trust option**. Then, select **Always Trust** for both **Secure Sockets Layer** (SSL) and **X.509 Basic Policy.**



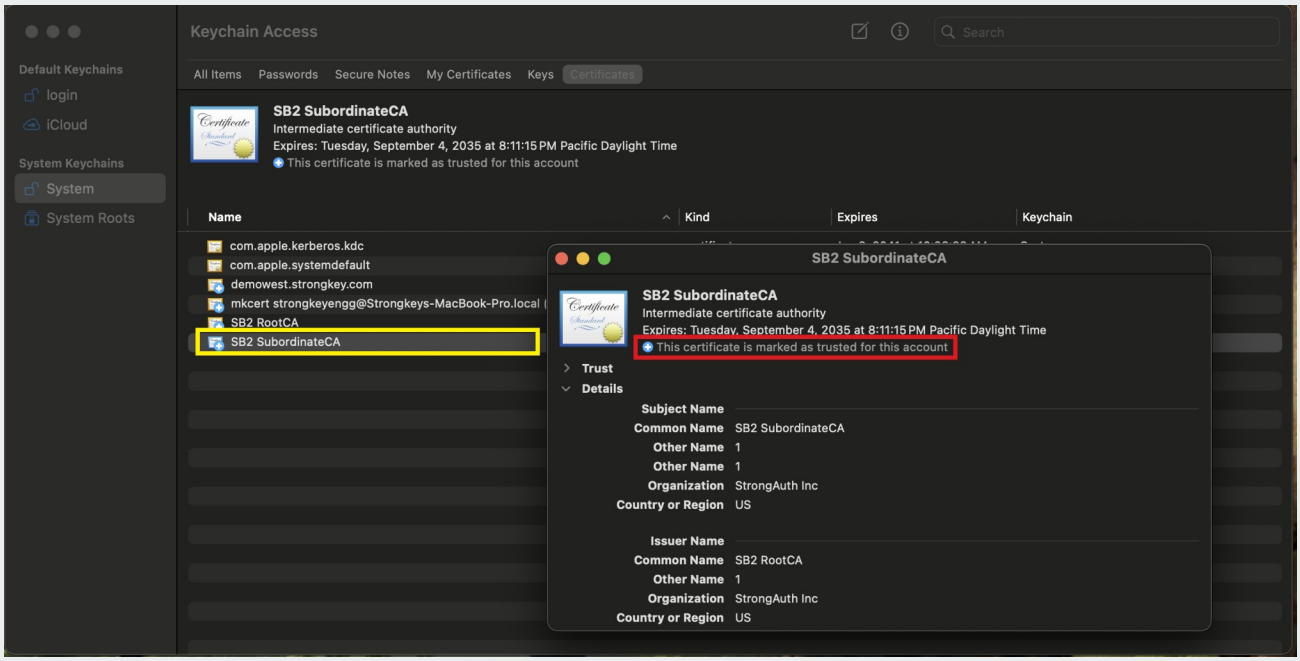
C8 Authenticating the Changes to the SB2 SubordinateCA Certificate

After the SB2 SubordinateCA **Get Info** window is closed, macOS prompts for authentication, using either **Touch ID** or the **macOS account password**, to confirm changes to the trust settings..



C9 Confirming the Trust Changes

To confirm the trust settings, **right-click** the SB2 SubordinateCA certificate and select **Get Info**. A successful import and trust is indicated by the message: ***"This certificate is marked as trusted for this account."***



SECTION D

D1 Accessing an SB2 Platform URL

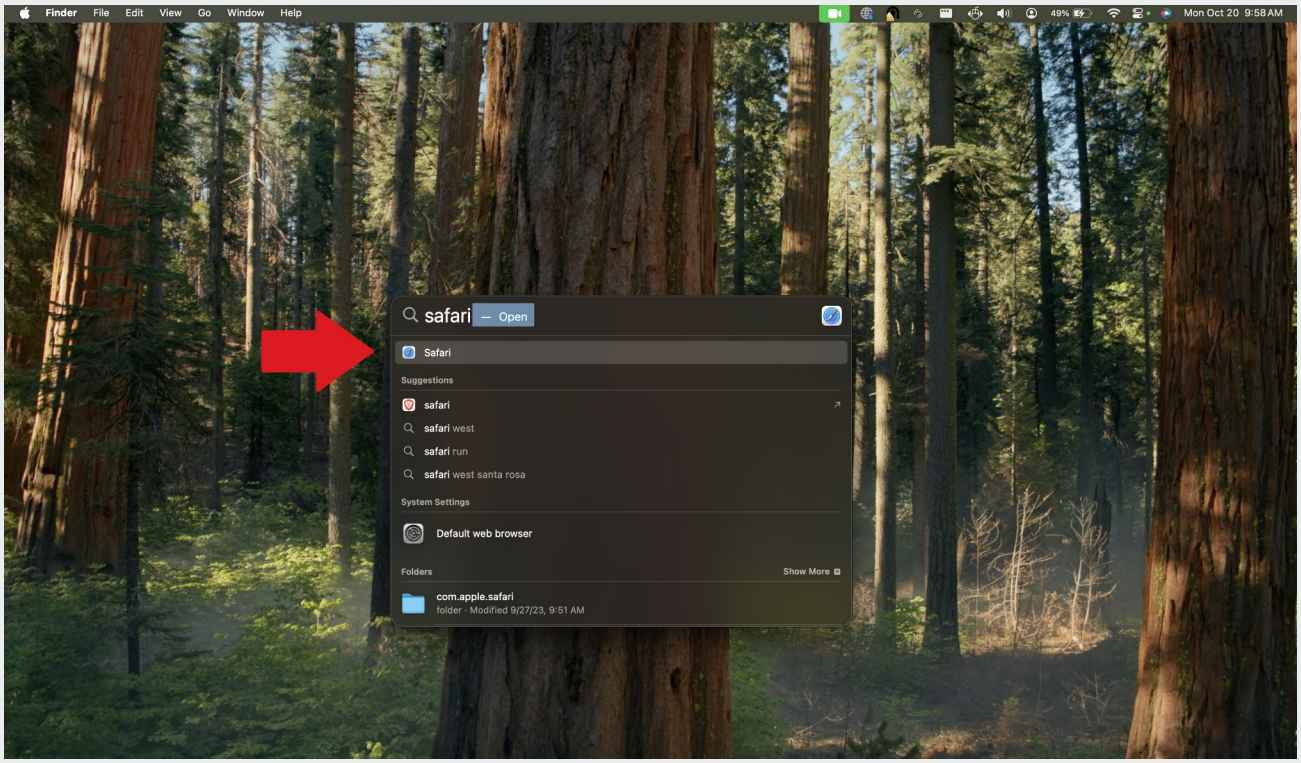
This section will review the steps of accessing an SB2 platform URL with a Yubikey 5C NFC Security Key.

D2 Prerequisites

- macOS 13 or above
- Safari
- Internet connection
- Yubikey 5C NFC Security Key – with the PIN to the Security Key
- SB2 Platform URL
- USB-C port or USB-C adapter

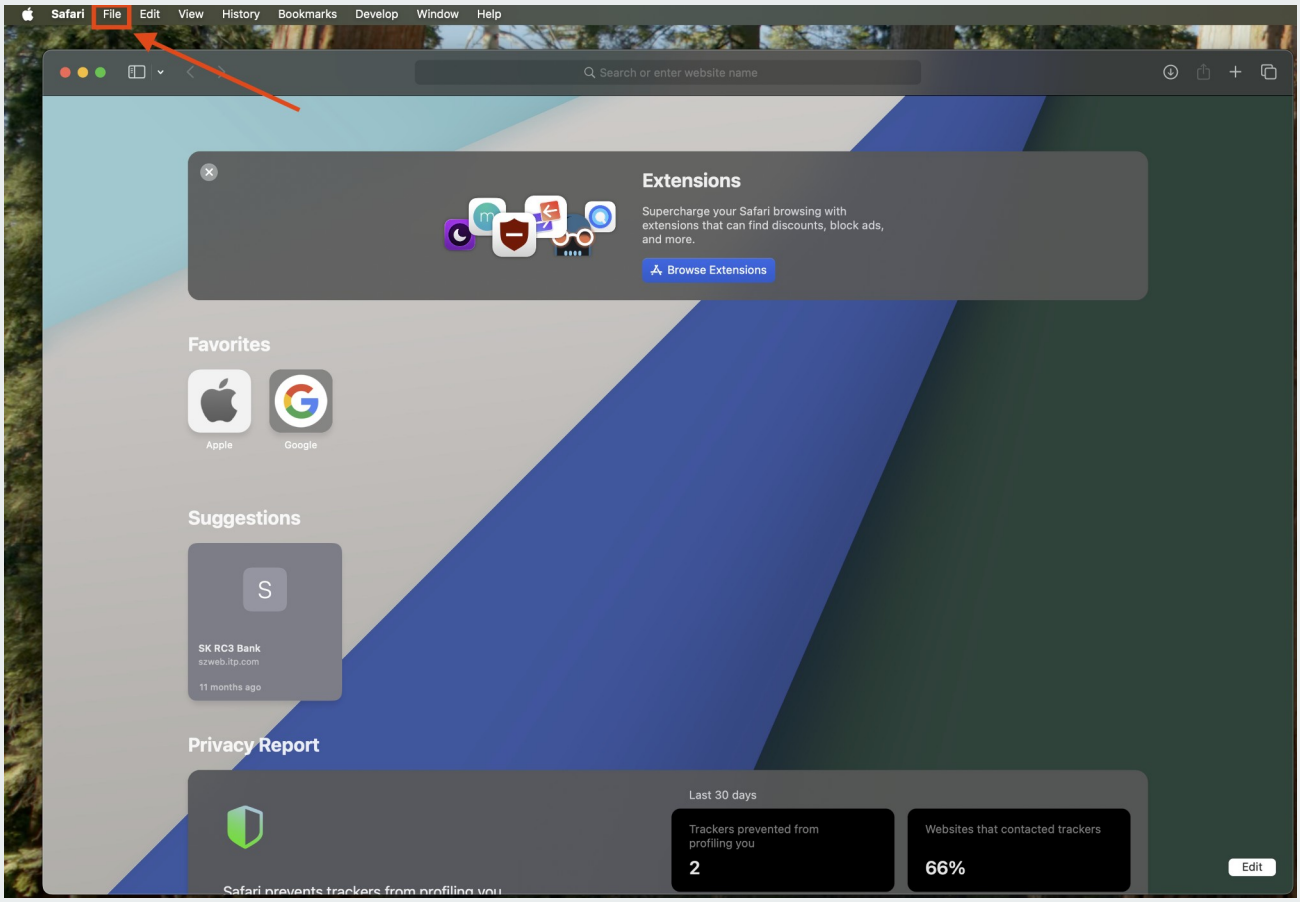
D3 Open the Safari Browser

To begin, access the Safari browser by searching with **Spotlight** [⌘ + Space].



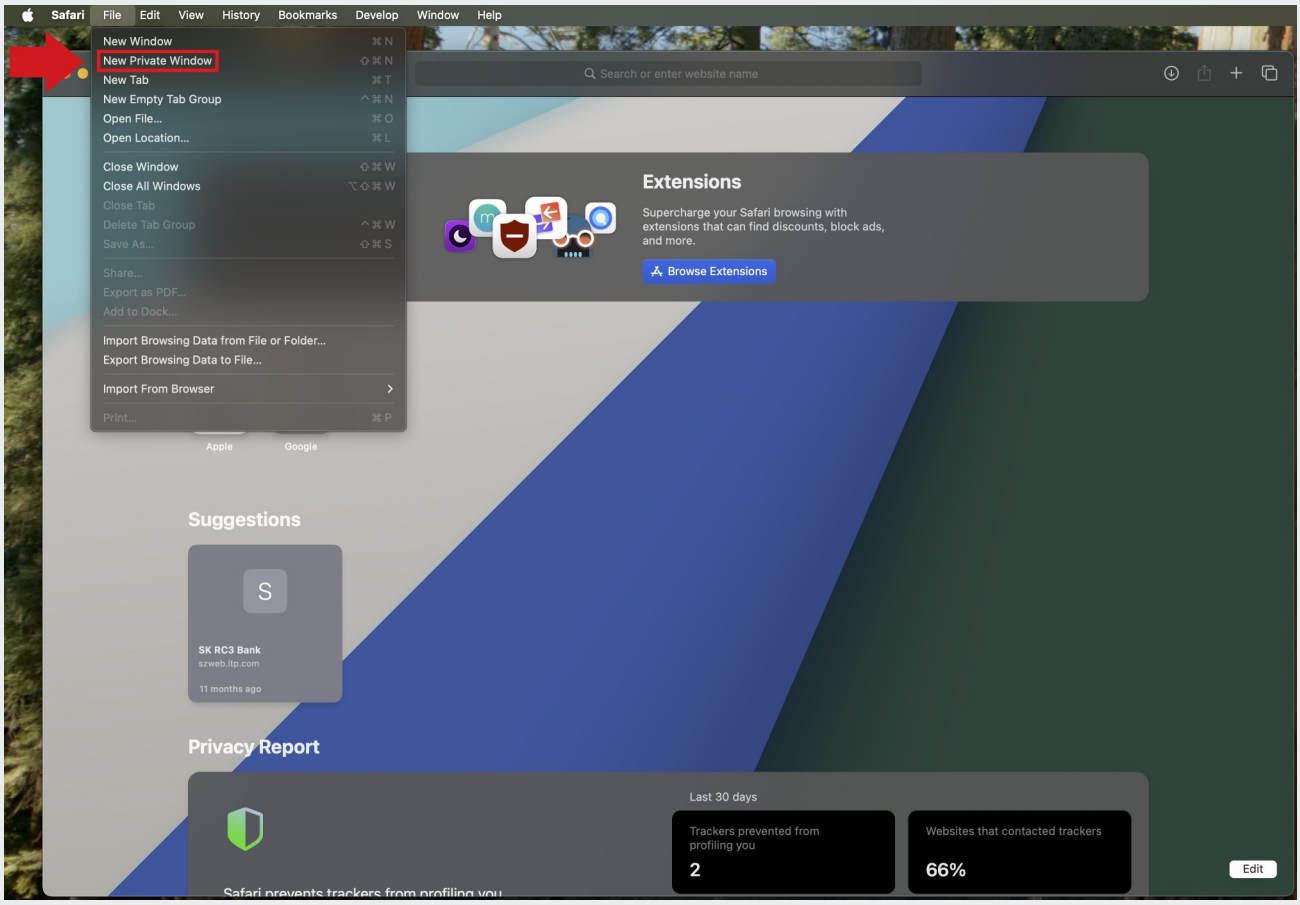
D4 Locate the File Menu

In the top-left corner of the menu bar, click the File menu to proceed.



D5 Open a New Private Window

To access the **SB2 platform**, open **Safari** and select **New Private Window** from the **File** menu.



D6 Plug in the Yubikey

Plug the **Security Key** into the USB-C port (or the USB-C to USB-A adapter)

D7 Identifying the USB-C port

Locate the USB-C port—typically found along the edge of the computer, it features a compact design with smooth, rounded corners that set it apart from traditional USB-A ports.
The image below shows both a USB-C port and its matching male connector.

D8 No USB-C port? No problem.

With the USB-A to USB-C adapter provided by the Administrator of your SB2 site, simply plug the USB-A end into the computer and insert the Security Key into the USB-C port.

The provided USB adapter pictured below.

D9 SB2 Platform URL

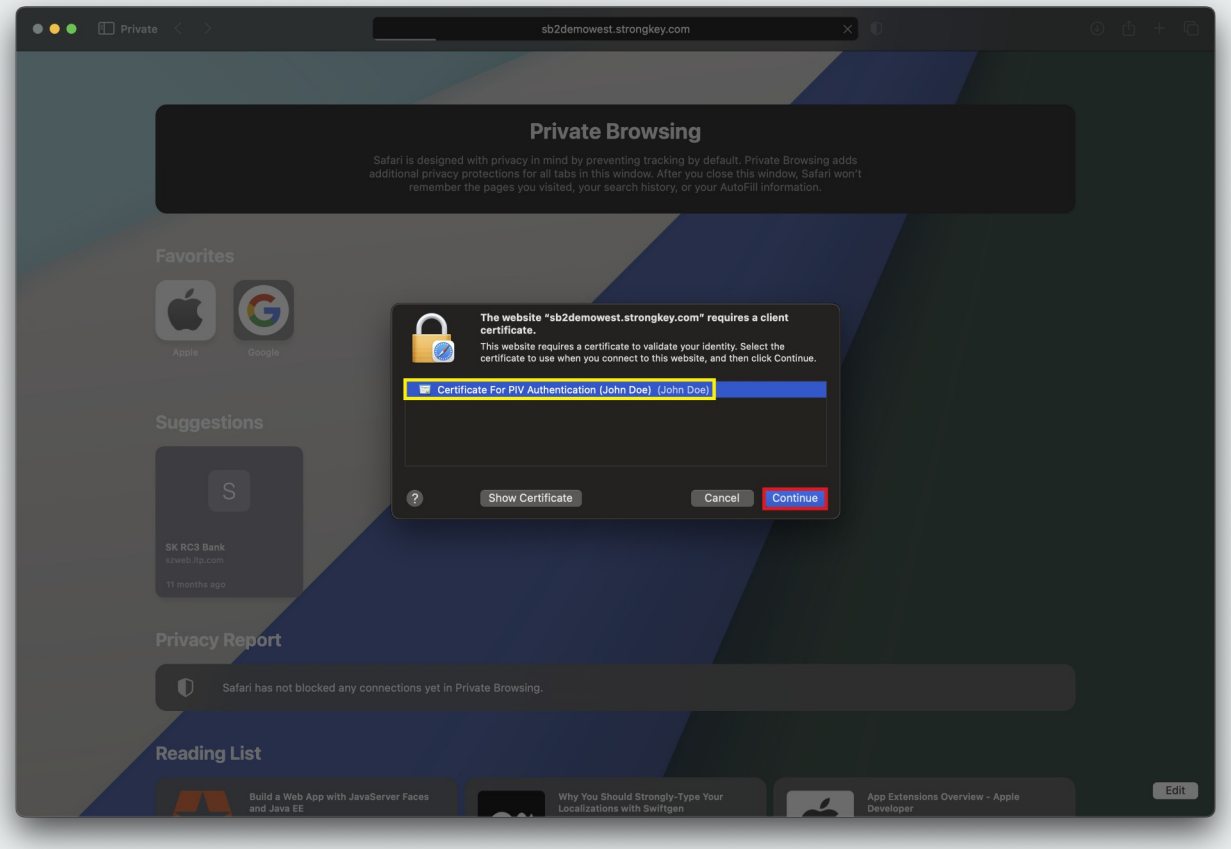
In the InPrivate browser address bar, enter the provided SB2 Demo invitation link. You will receive the link in an email from a member of the StrongKey Team. **Please note**, the URL is long so it will be advantageous to use the "cut and paste" options. Here is an example of what the URL will look like:

- https://sb2demo.strongkey.com:443/sb2/register?hash=3d500dec79f6ec257ebddcc56hj78ff1f2d31d557d4c7bf5654

D10 Select the Certificate

A pop-up window will display the available certificates. The name in the prompt should match your name, as created by the Administrator of the SB2 platform site. Select the presented certificate and **click OK** to proceed.

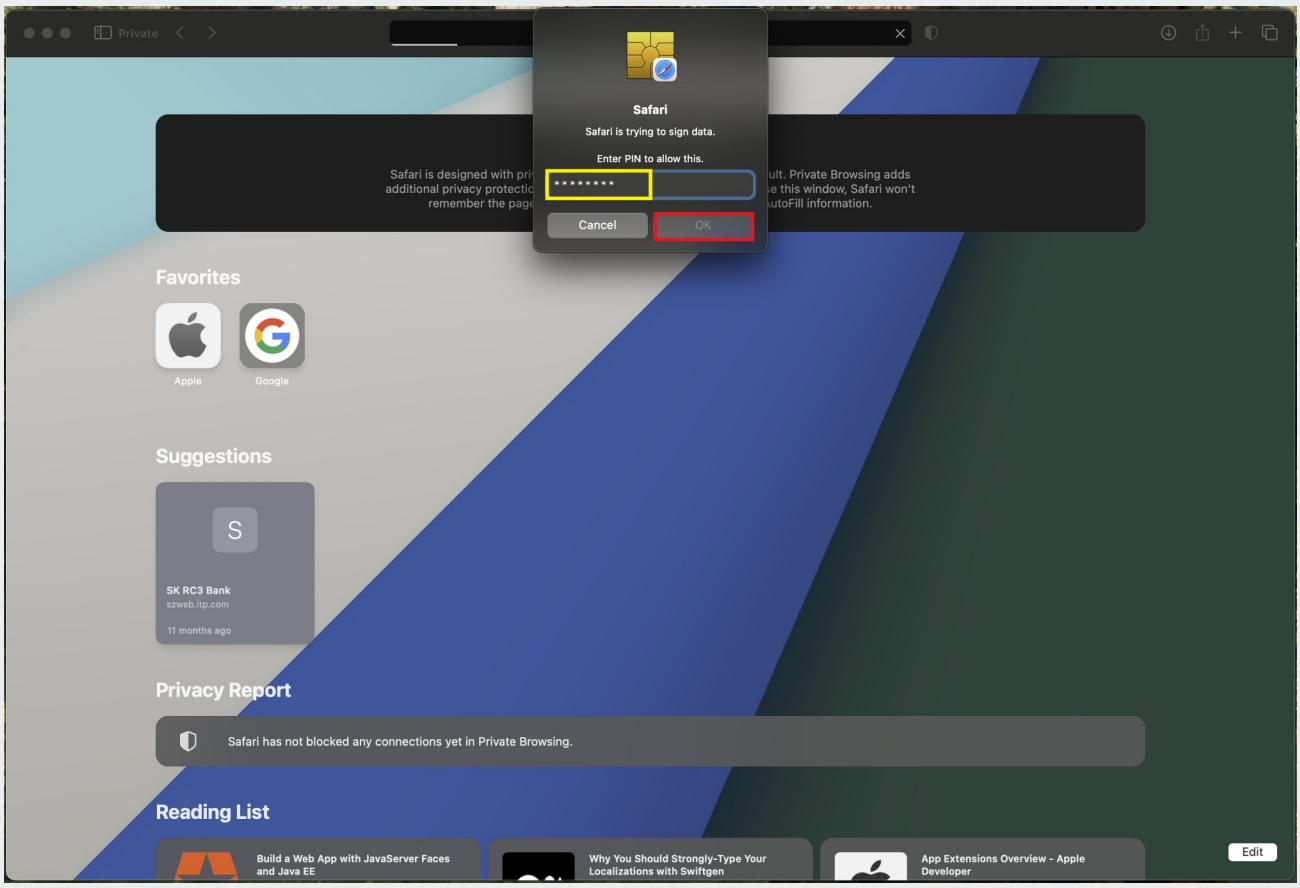
NOTE: A certificate prompt appears when the **SB2 Root CA** and **SB2 Subordinate CA** certificates are imported successfully on the system. If a prompt is not displayed, contact the SB2 platform administrator for assistance.



D11 Enter Security Key PIN

The next dialog box will prompt for the Yubikey 5C NFC (aka Smartcard) **PIN**. Enter and **click OK** to continue. This PIN should have been provided by the Administrator of the SB2 platform site.

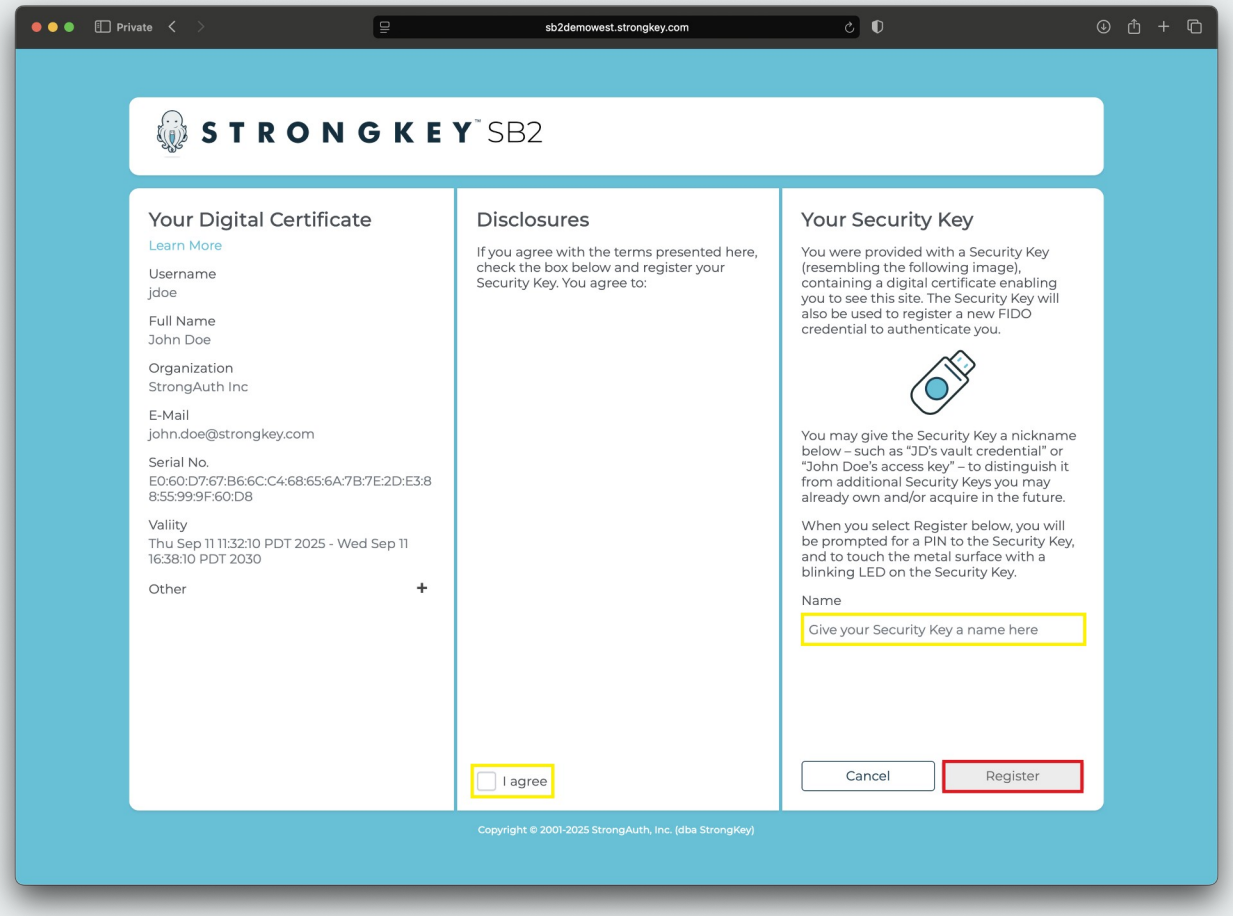
For instructions on changing the Yubikey PIN, refer to the appendix of this guide.



D12 SB2 Landing Page

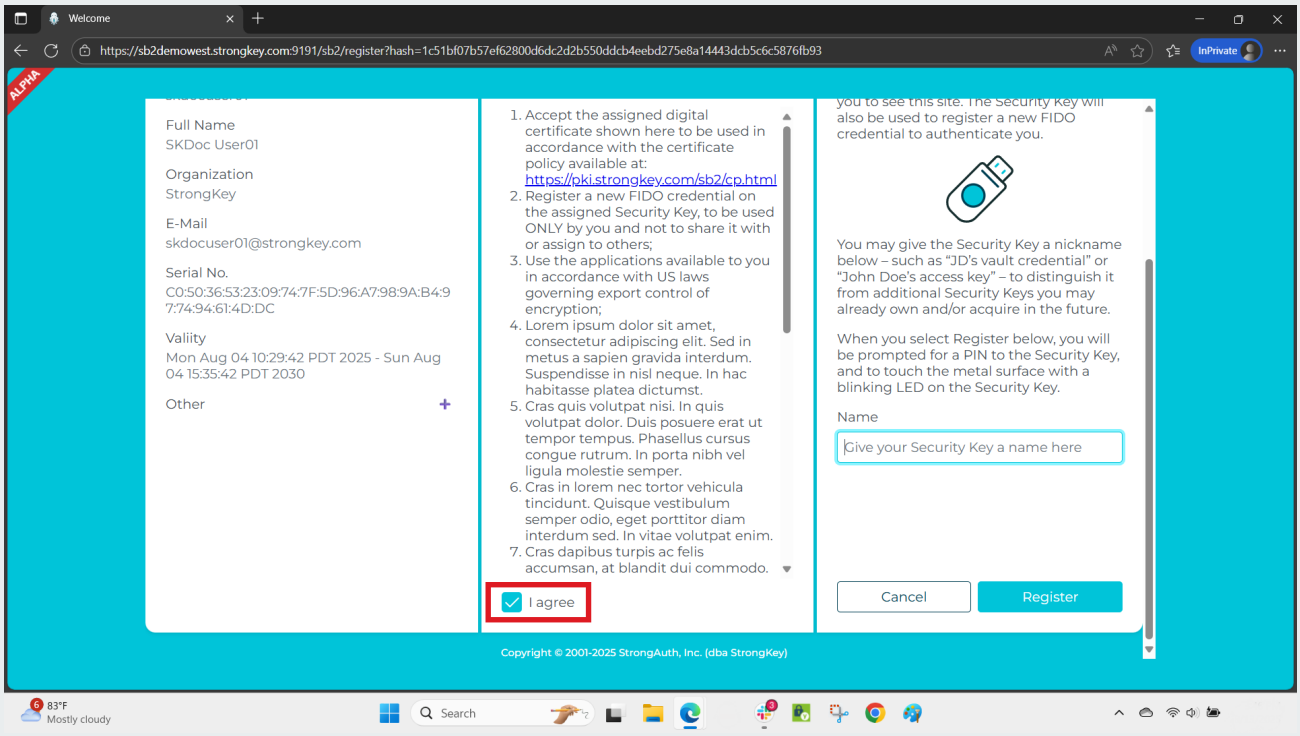
Upon successful authentication with the digital certificate, the following one-time **SB2 Platform Landing Page** will be displayed. This page has three (3) sections:

- On the left, key details about the digital certificate are displayed.
- The middle panel presents important legal disclosures from the SB2 platform. Review is required—after scrolling to the bottom and agreeing to the terms, you can proceed.
- In the right panel, a nickname can be assigned to the Security Key, for easier identification among multiple keys.



D13 Terms and Conditions

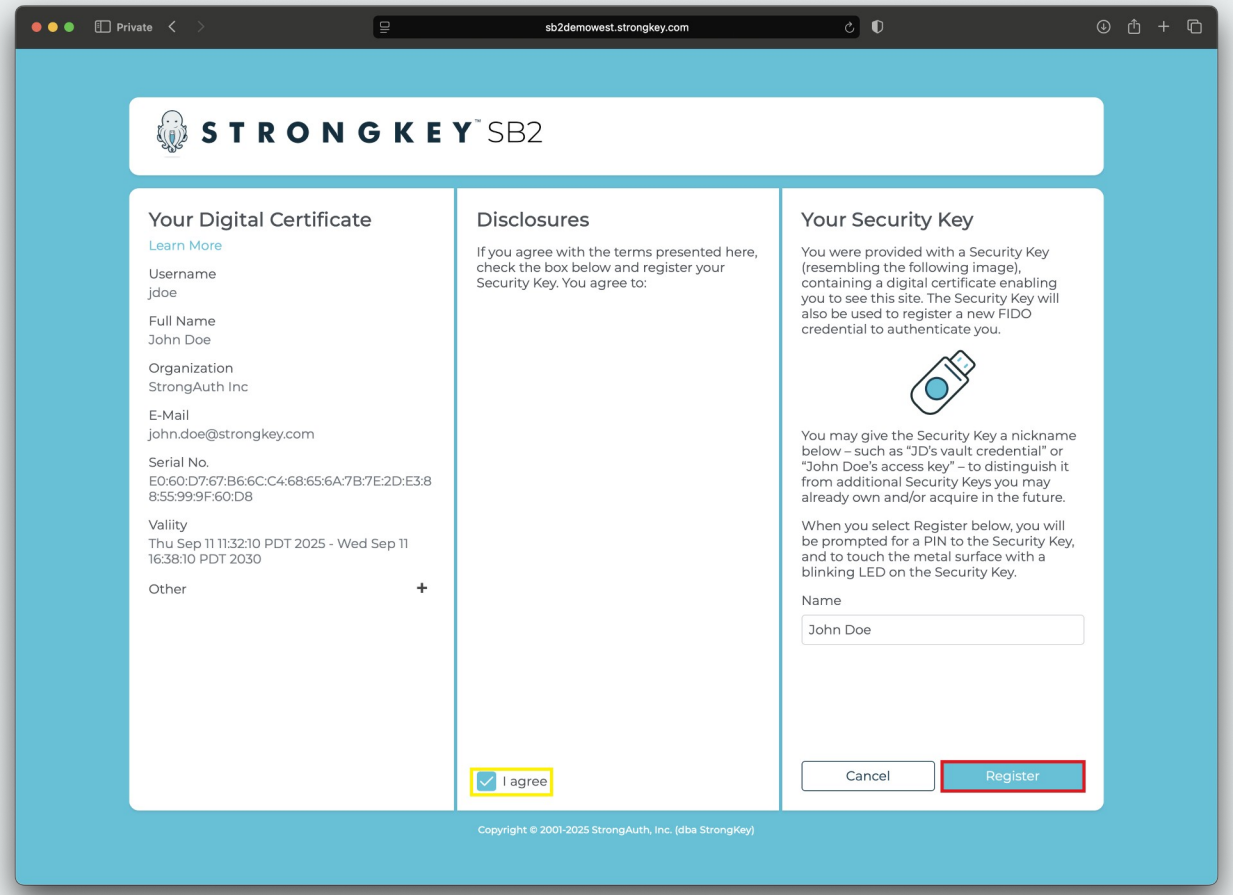
Review and accept the terms and conditions in the **Disclosures** panel. The **"I agree"** box must be checked before proceeding with **Security Key** registration.



D14 Give the Security Key a Name

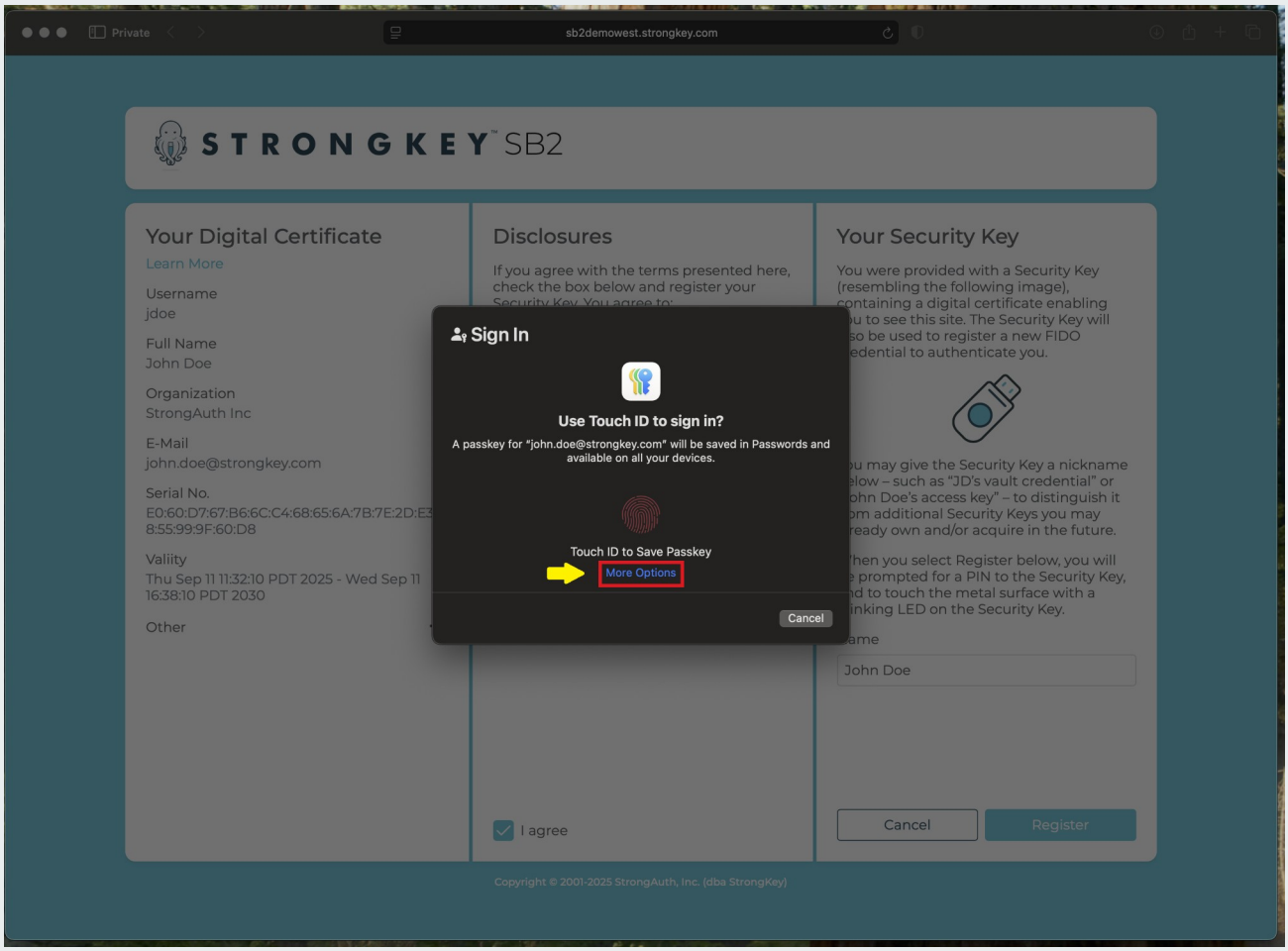
In the Security Key panel on the right, enter a descriptive nickname for the key in the **Name** field. Then select **Register** to complete the process. Names are typically short (up to 16-20 alpha-numeric characters), such as:

- John's SB2 key at mysite.com
- Yubikey for mysite.com SB2



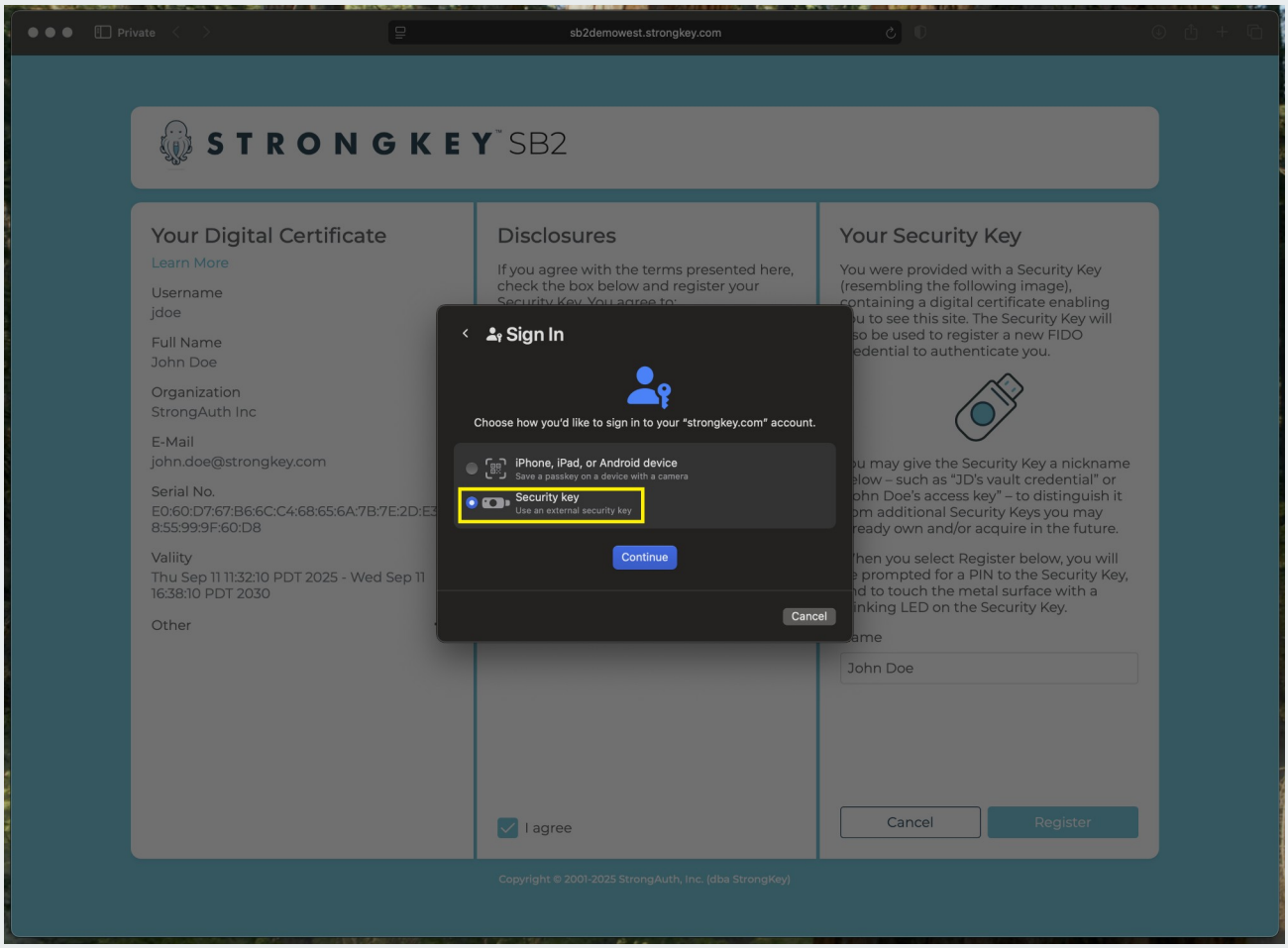
D15 Continue Setup

A dialog box will appear to confirm continuation of the setup process, authorizing the current device to also access the SB2 platform website. Select **More Options** to proceed.



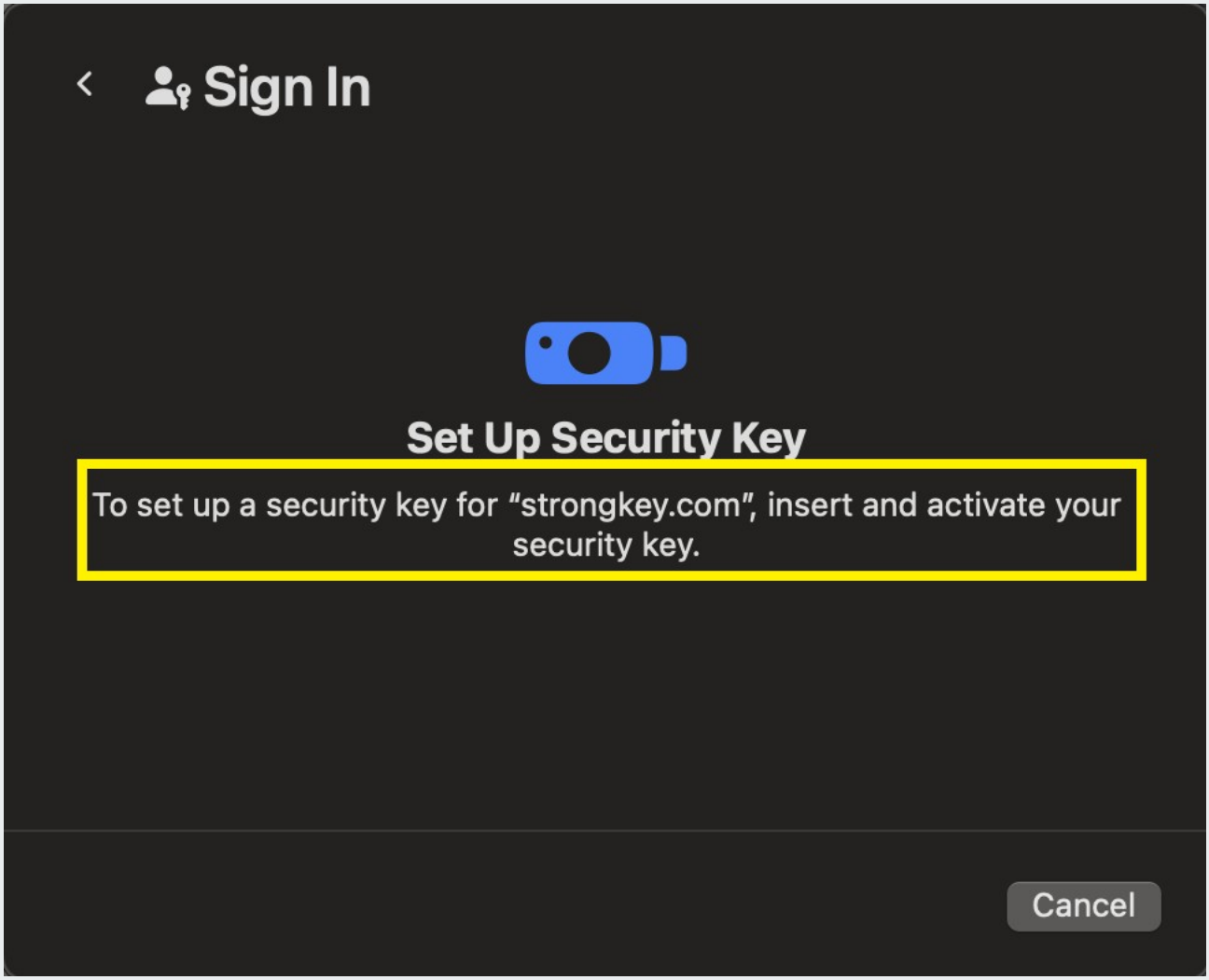
D16 Select Security Key

Next, select the **Security Key** for location of where the credential is stored. It is important to verify this location as the Security Key. **Click Continue** to proceed.



D17 Security Key Setup

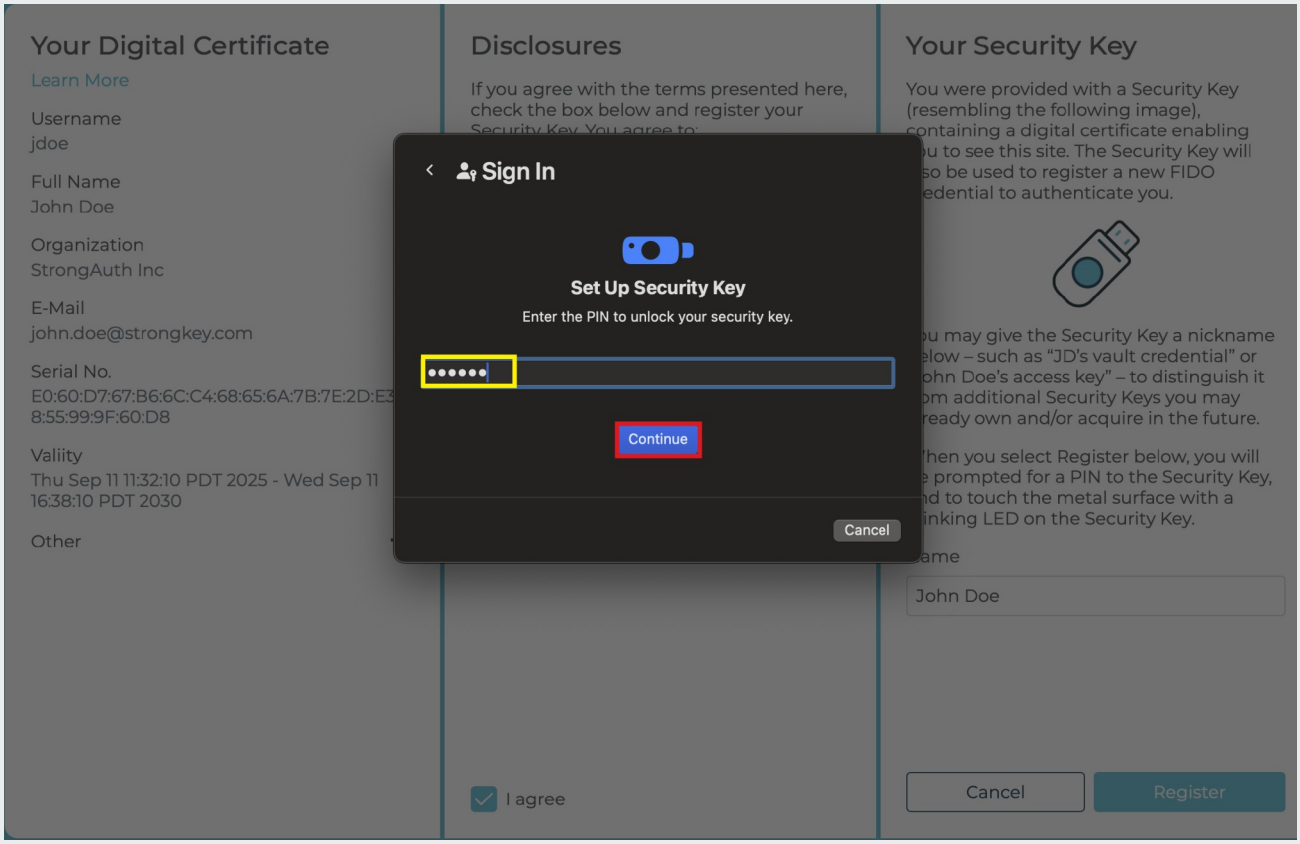
A confirmation dialog box will appear to verify the Security Key is being configured for SB2 platform login. To proceed, please activate the security key by touching the metal contact visible on the **Security Key** with your finger - it will have a light-emitting diode (aka LED) blinking to indicate where it must be touched.



D18 Enter Security Key PIN

To continue adding a credential to the **Security Key**, enter the PIN and **click Continue**.

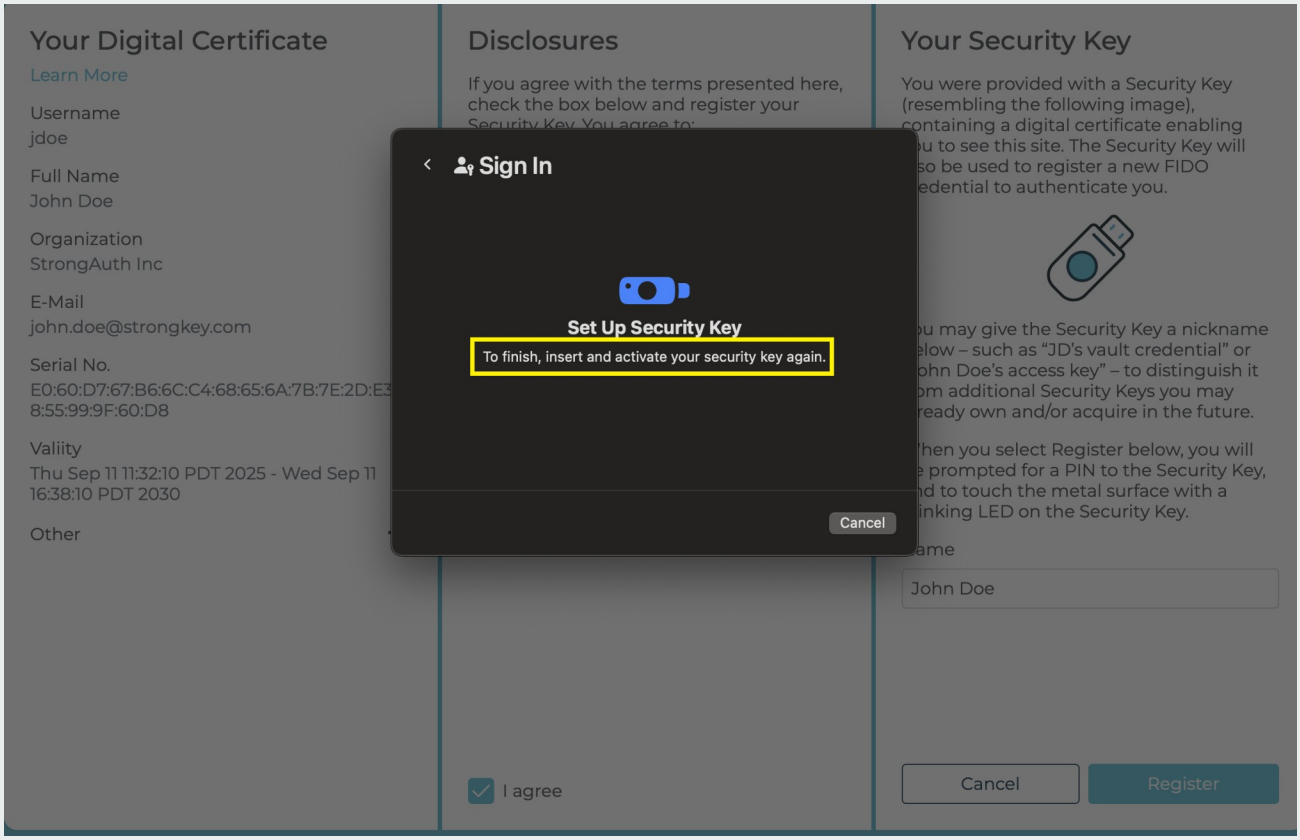
NOTE: This step in the process is known as the "**User Verification**" (aka UV) in the FIDO ecosystem. It is a security feature of the FIDO authentication protocol to ensure that the SB2 platform can verify the legitimate owner's PIN of the **Security Key**. SB2 sites will mandate a security policy where the PIN to the **Security Key** is not shared with others. Every time the FIDO credential is used to authenticate you to the SB2 platform, you will be required to perform the UV function as a security precaution.



D19 Touch the Security Key

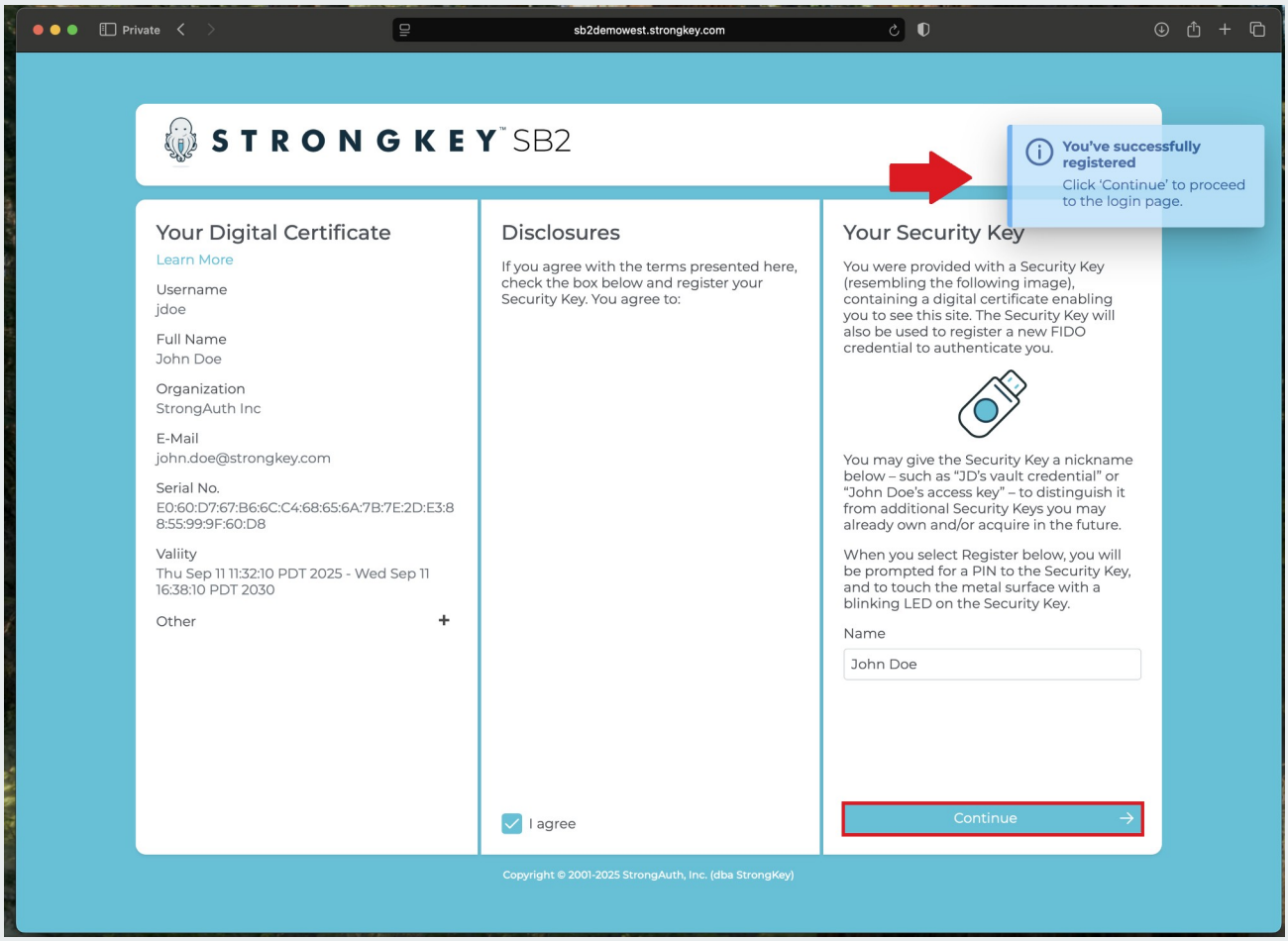
To continue the setup, touch the Security Key.

NOTE: This step in the process is known as the "**Test of User Presence**" (aka TUP) in the FIDO ecosystem. It is a security feature of the FIDO authentication protocol to ensure that a remote attacker can never steal your identity from a remote computer since they will neither have a **Security Key** with your FIDO credential nor will they be able to perform the "test of user presence" at your computer (where the FIDO transaction is occurring). Every time the FIDO credential is used to authenticate you to the SB2 platform, you will be required to perform the TUP as a security precaution.



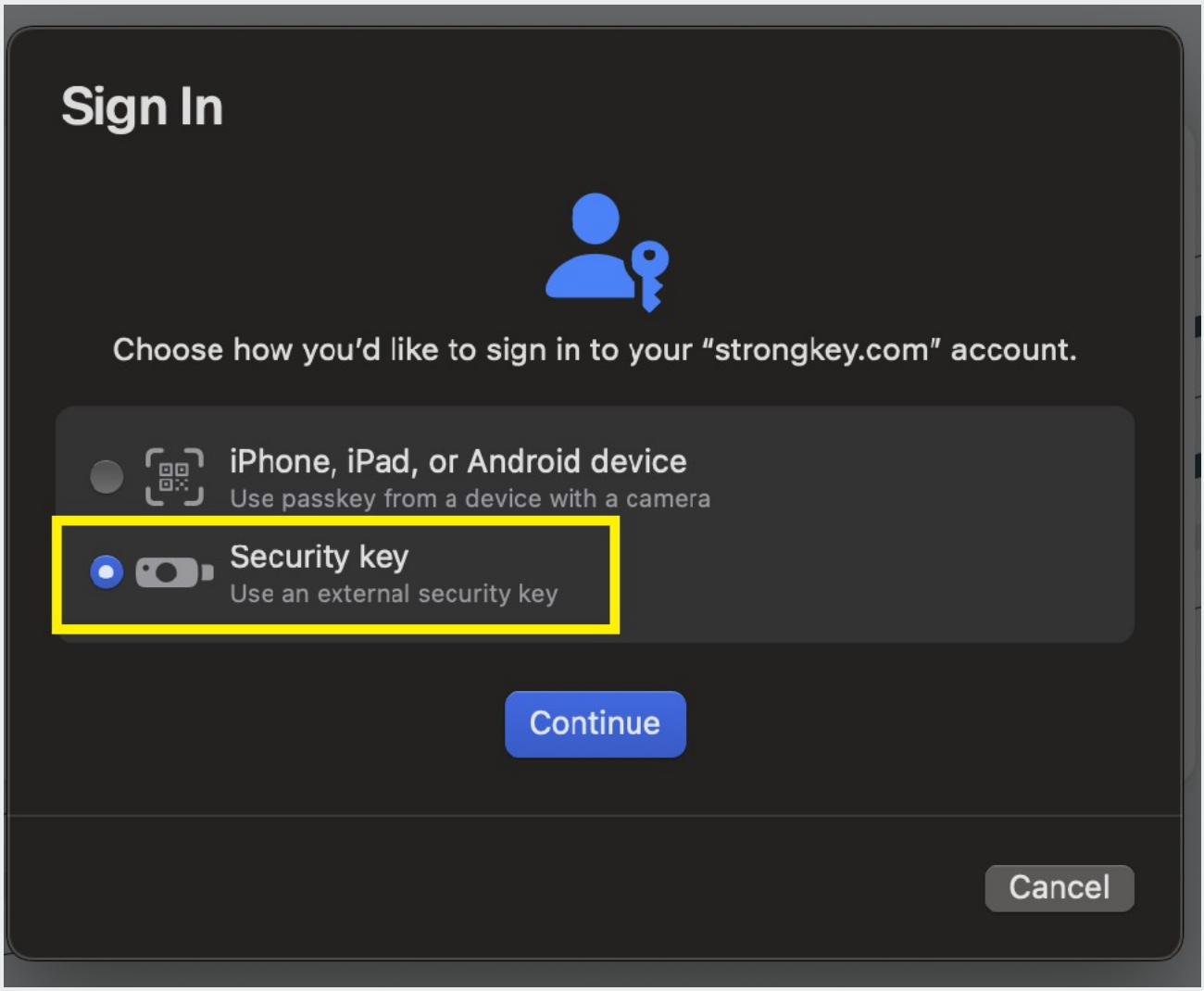
D20 SB2 Confirmation

After touching the security key, SB2 will flash a blue message confirming successful registration.



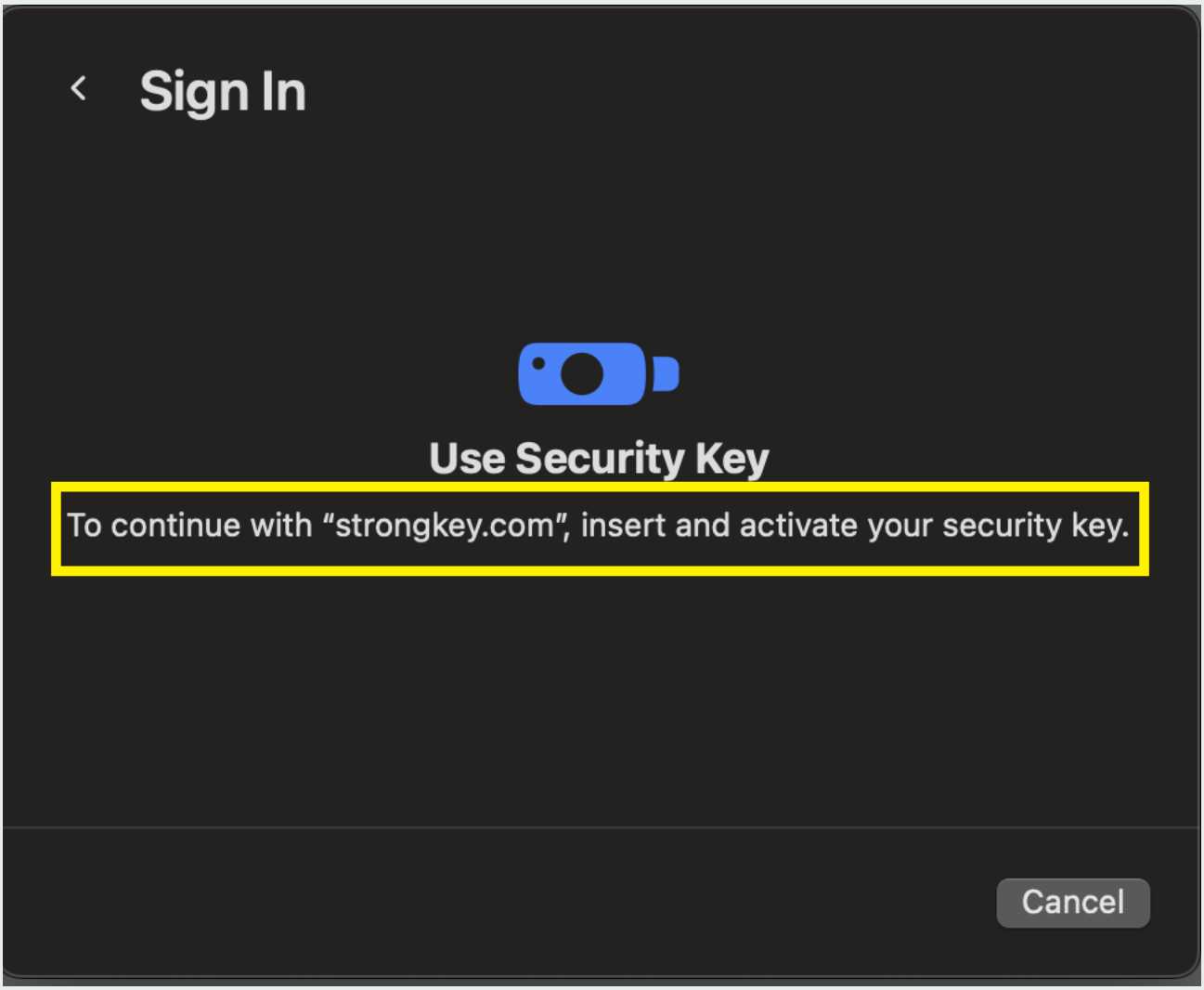
D21 Signing In

After clicking **Continue**, a prompt will appear prompting you to sign in with the new credential. Make sure you choose the **Security Key** when authenticating to the SB2, and **click Continue.**



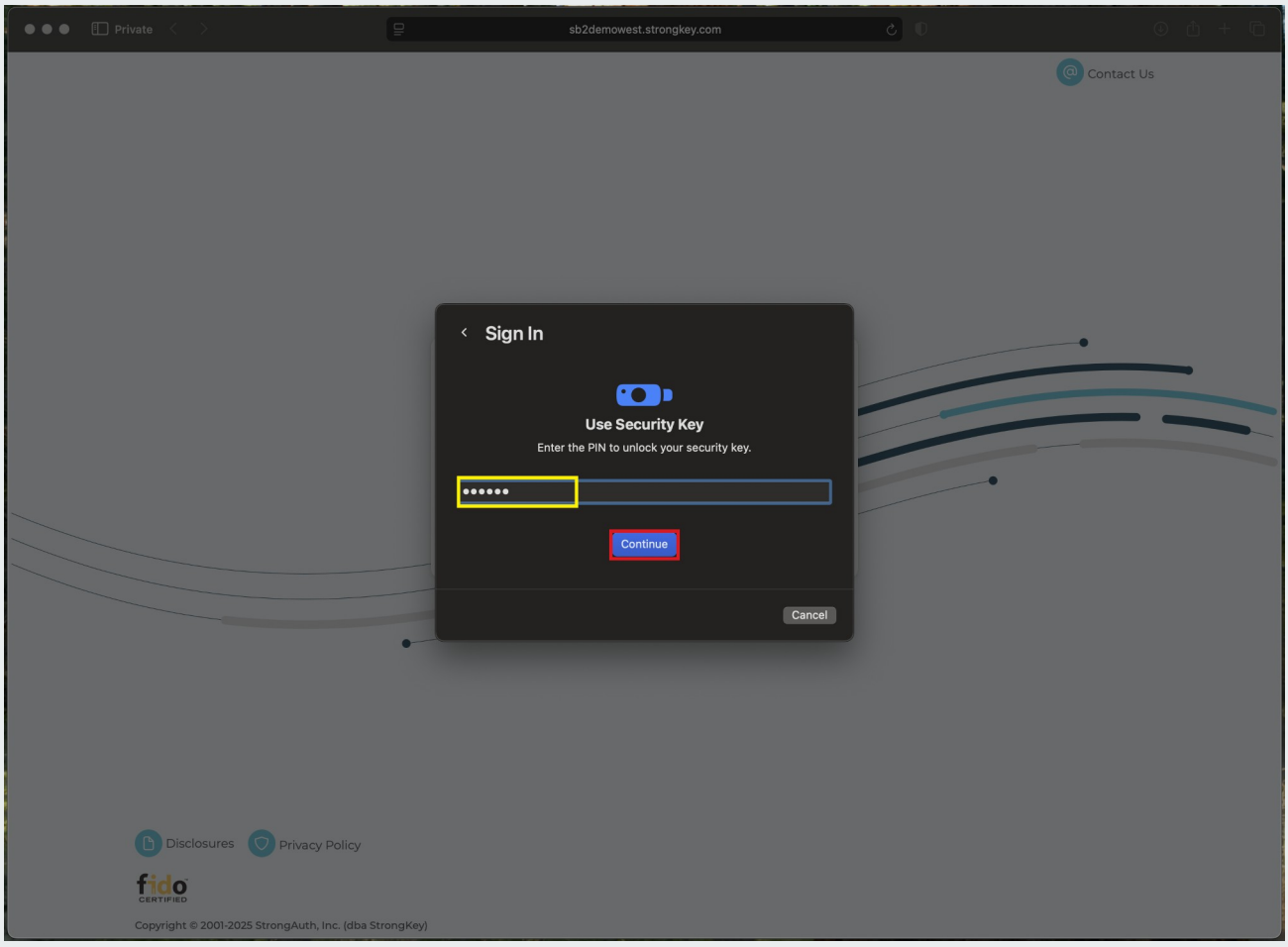
D22 Select Security Key

The next dialog box will ask you to activate the security key by **touching** the metal contact on top of the **Security Key** where an LED is blinking.



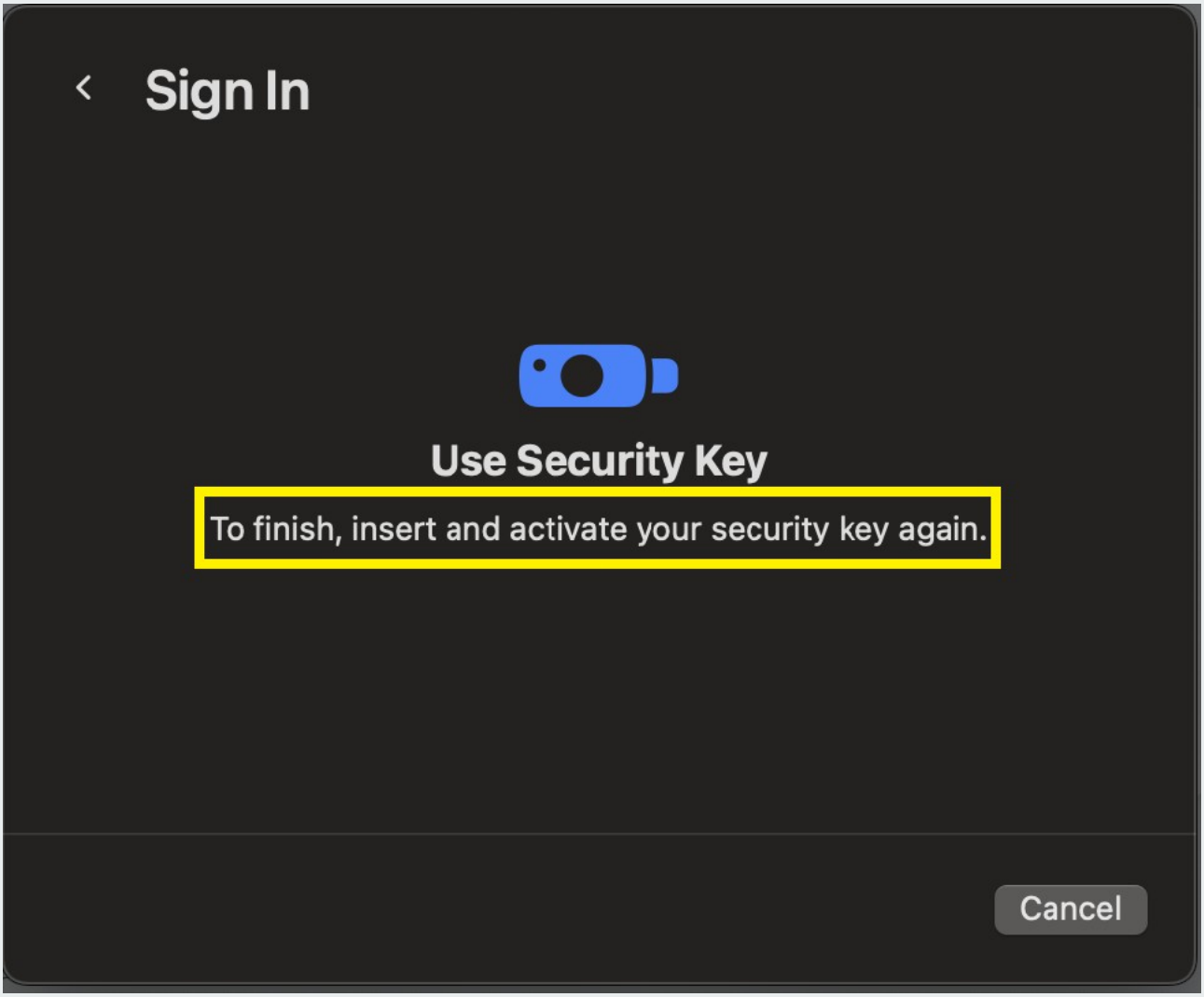
D23 User Authentication

The next dialog box will verify the user. Enter the **PIN** to the **Security Key** and **click Continue**.



D24 Test of User Presence

To continue the login procedure, touch the metal contact on top of the **Security Key** where an LED is blinking – this confirms a user is present and attempting to sign in from that computer with a legitimate credential on the **Security Key**.

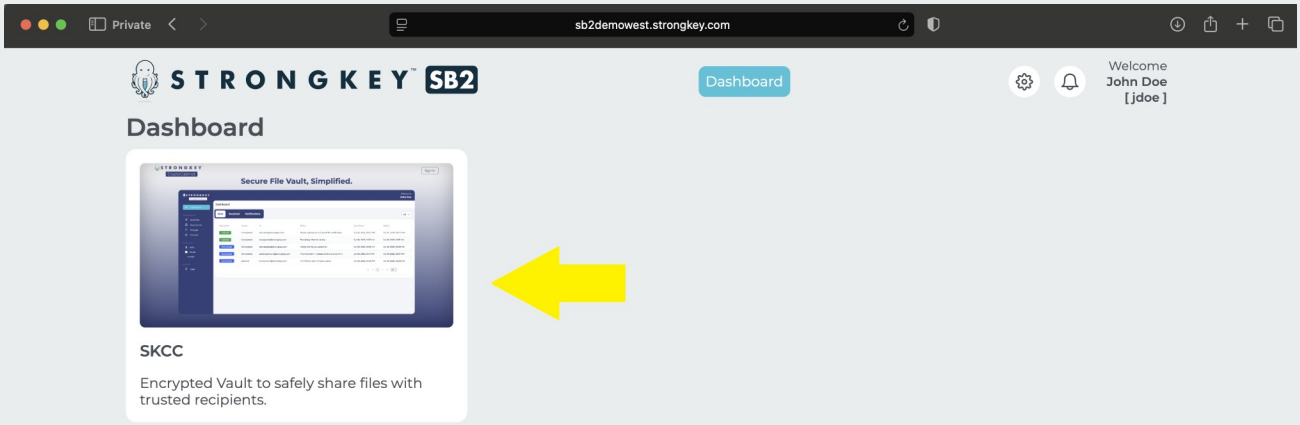


D26 SB2 Platform Dashboard

CONGRATULATIONS!

The SB2 Platform is now accessible, and the Security Key with the registered FIDO credential has been successfully configured. You'll see your account name displayed on the right side of your screen. To update your profile, simply click the **gear** icon.

All SB2 users may use the **StrongKey CryptoCabinet** (SKCC) web application for secure storage and sharing files. To access SKCC, click the application image on the SB2 Dashboard—this will open the SKCC Dashboard in a new browser tab. StrongKey will provide comprehensive, step-by-step instructions on using SKCC shortly.



Appendix

STRONGKEY™

Changing a Yubikey Personal Identification Number (PIN)

AP1 Changing a Yubikey 5C NFC Personal Identification Number (PIN)

The **Security Key** is a very powerful cybersecurity device and represents the state-of-the-art in multi-factor authentication (MFA) technology that does not use any passwords. The MFA is supported by the:

- **Possession factor** – where the physical possession of the Security Key is essential to the authentication process;
- **Knowledge factor** – where know the PIN to the Security Key is also essential to the authentication process.

Since the **Security Keys** provided with the SB2 use two different NIST-approved, passwordless authentication protocols, there are two containers for the cryptographic keys used with the protocols. Each container is managed by a separate PIN.

However, StrongKey recommends using the SAME PIN to both containers of the **Security Key** to reduce the burden on users. As long as the **Security Key** is safely in the possession of the legitimate user, and the legitimate user is NOT sharing the PIN to the **Security Key** with anyone, the user will be complying with one of the strictest security policies recommended for access control.

This document outlines the process for changing the two required PINs – one for the digital certificate and the other for the FIDO credential.

AP2 Prerequisites

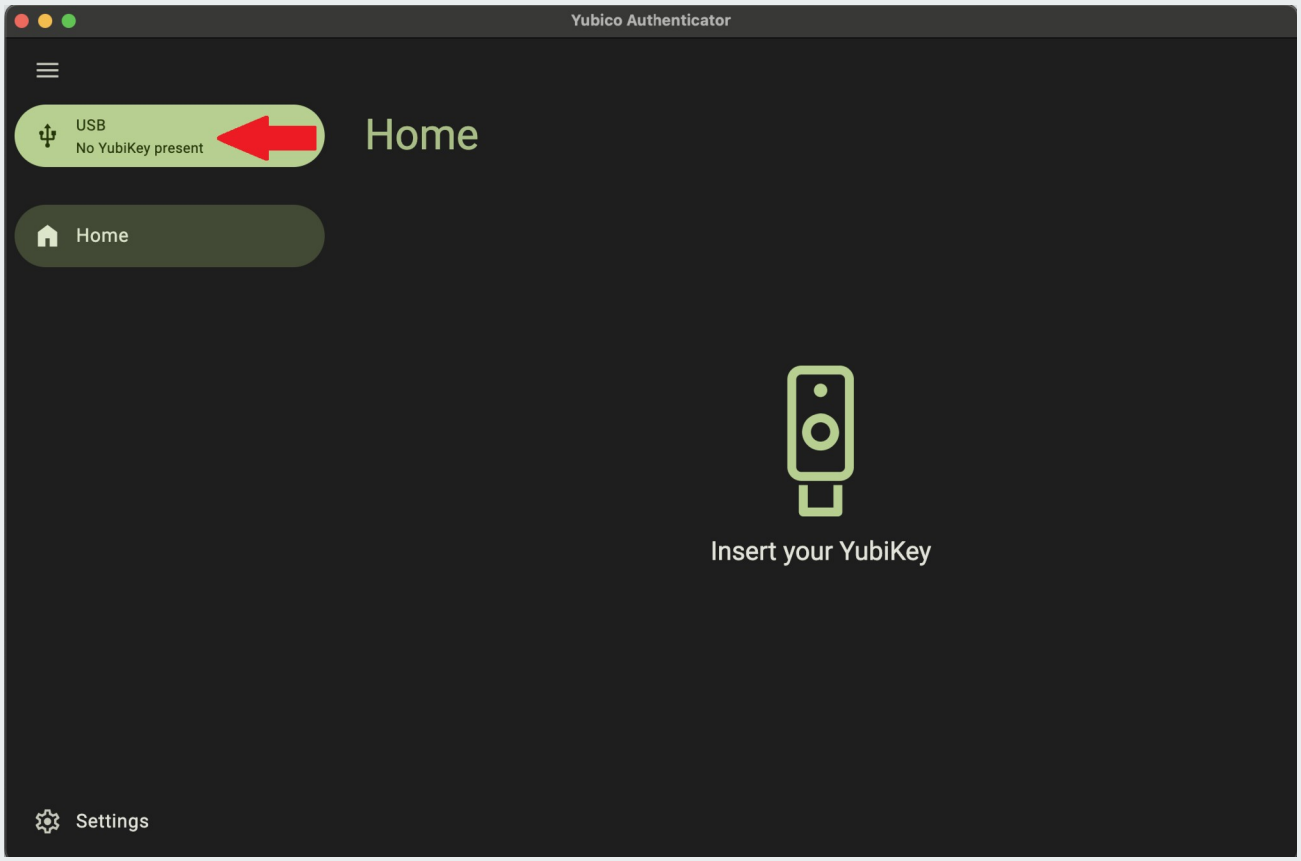
- macOS 13 or above
- USB-C port or USB-C adapter
- Yubico Authenticator application

AP3 Open the Yubico Authenticator Application

To begin, open the **Yubico Authenticator** application by searching for it with **Spotlight** (⌘ + Space) or locating it in **Finder's** Applications folder.

AP4 The Yubico Authenticator application

Upon opening, the Authenticator application displays the screen shown below and indicates there is **No Yubikey Present.**



AP5 Insert the Yubikey

Plug the **Security Key** into the USB-C port.

AP6 Identifying the USB-C port

Locate the **USB-C port**—typically found along the edge of the computer, it features a compact design with smooth, rounded corners that set it apart from traditional USB-A ports. The image below shows both a USB-C port and its matching male connector.

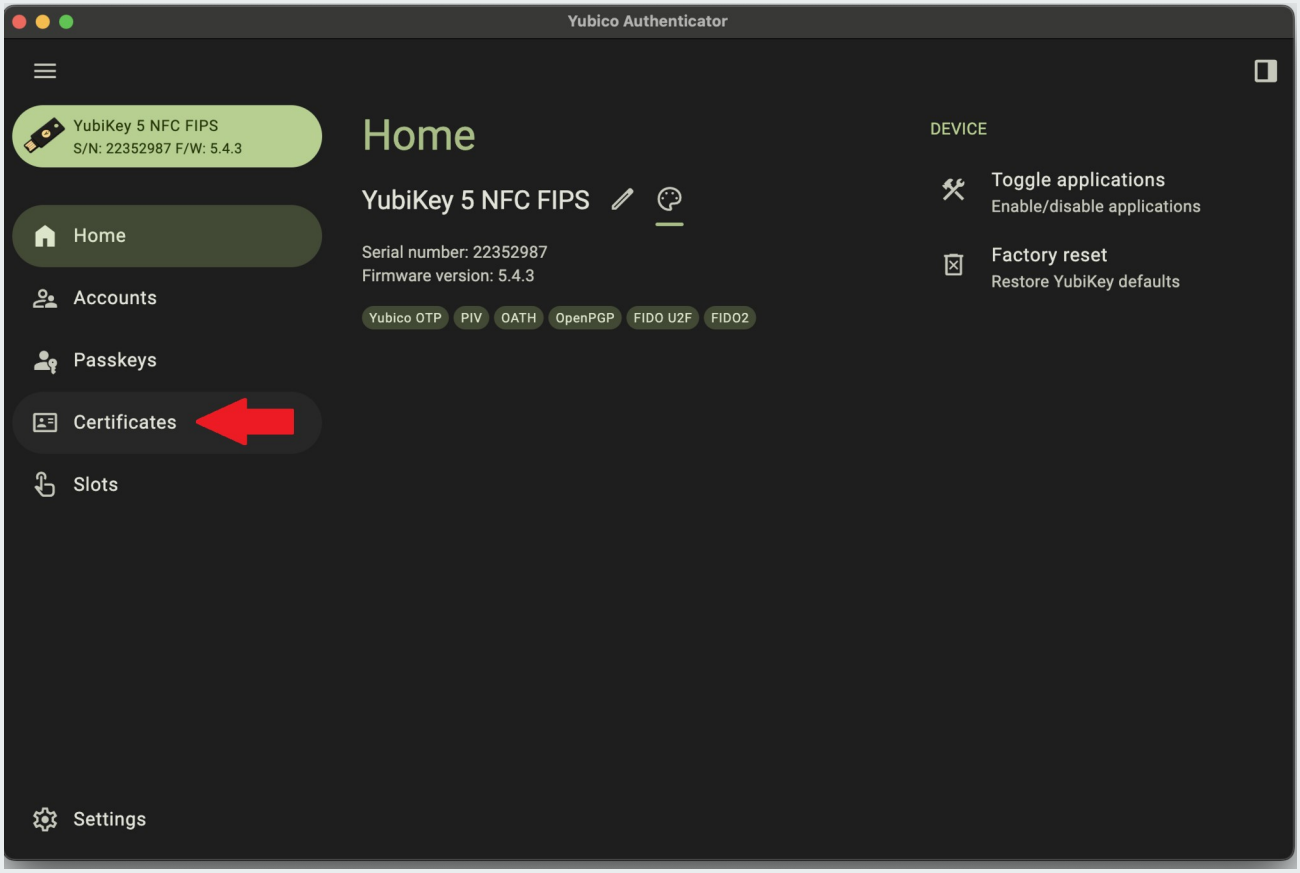
AP7 No USB-C port? No problem.

With the provided **USB-A to USB-C adapter**, simply plug the USB-A end into the computer and insert the **Security Key** into the USB-C port.

The provided USB adapter pictured below.

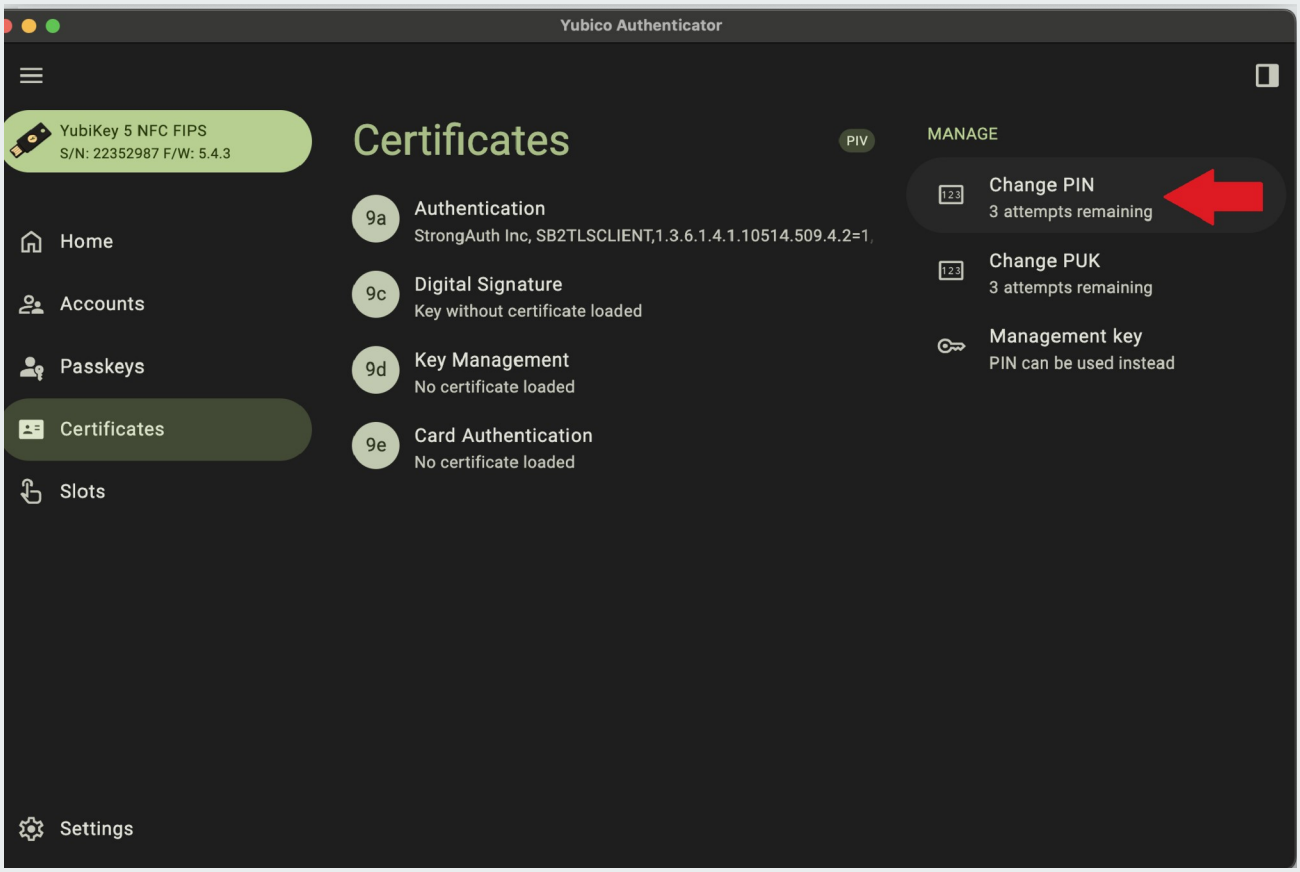
AP8 Changing the Digital Certificate PIN

From the home screen, navigate to the left and select the **Certificates** option from the menu.



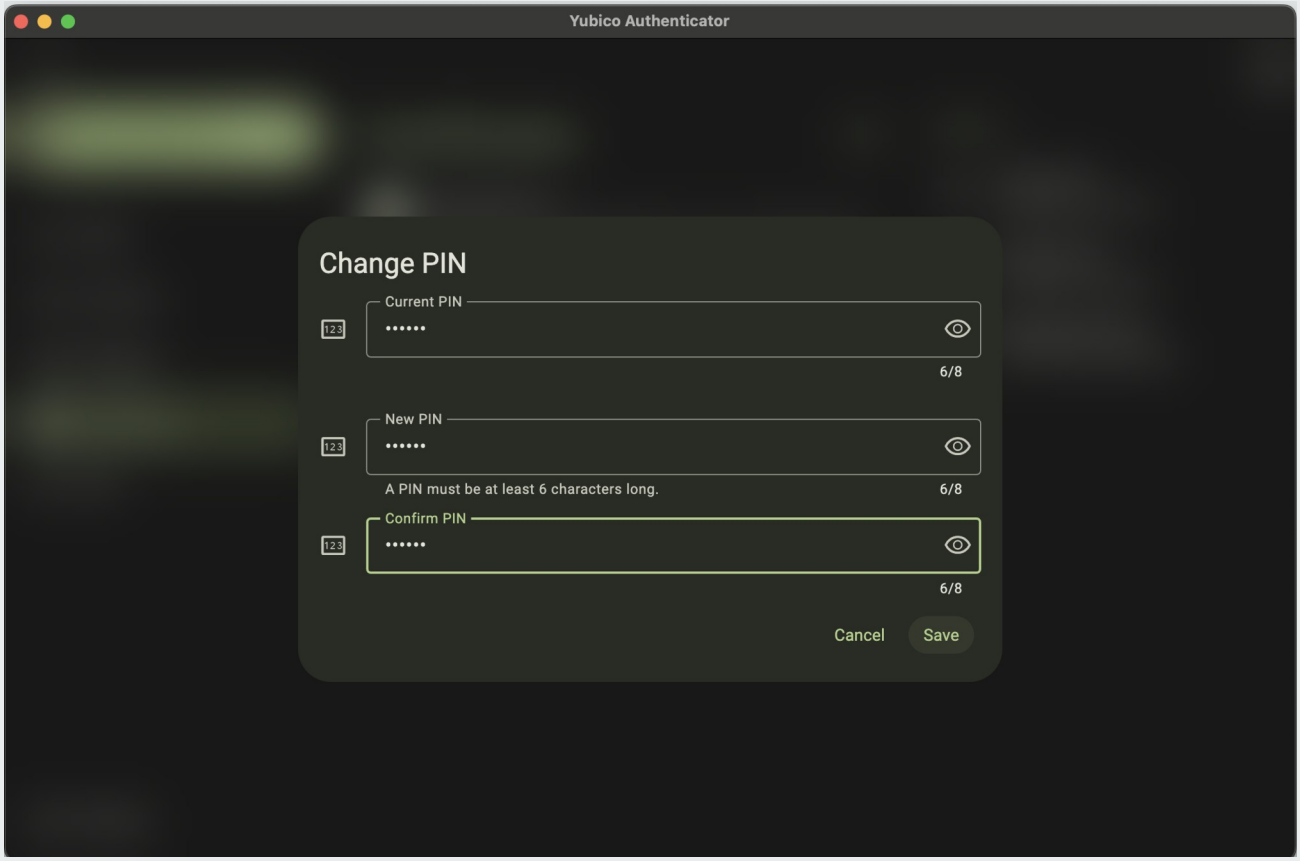
AP9 Change PIN option

Select the **Change PIN** option from the **Manage** menu on the right.



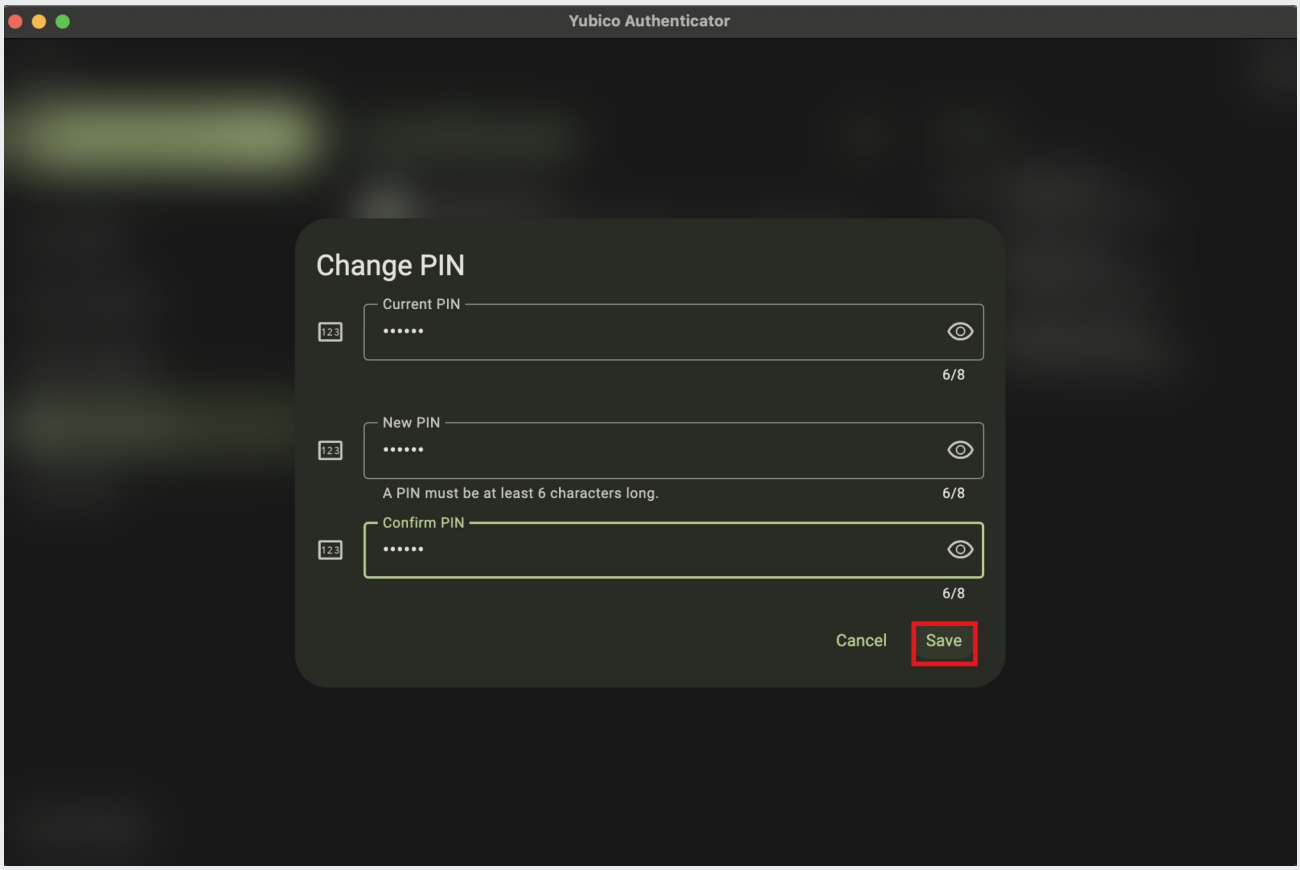
AP10 Enter PIN information

- In the top field, enter the **default PIN: 123456**.
- Enter the new PIN in the middle field. The PIN must contain 6 to 8 characters.
- Re-enter the new PIN in the final field to confirm.



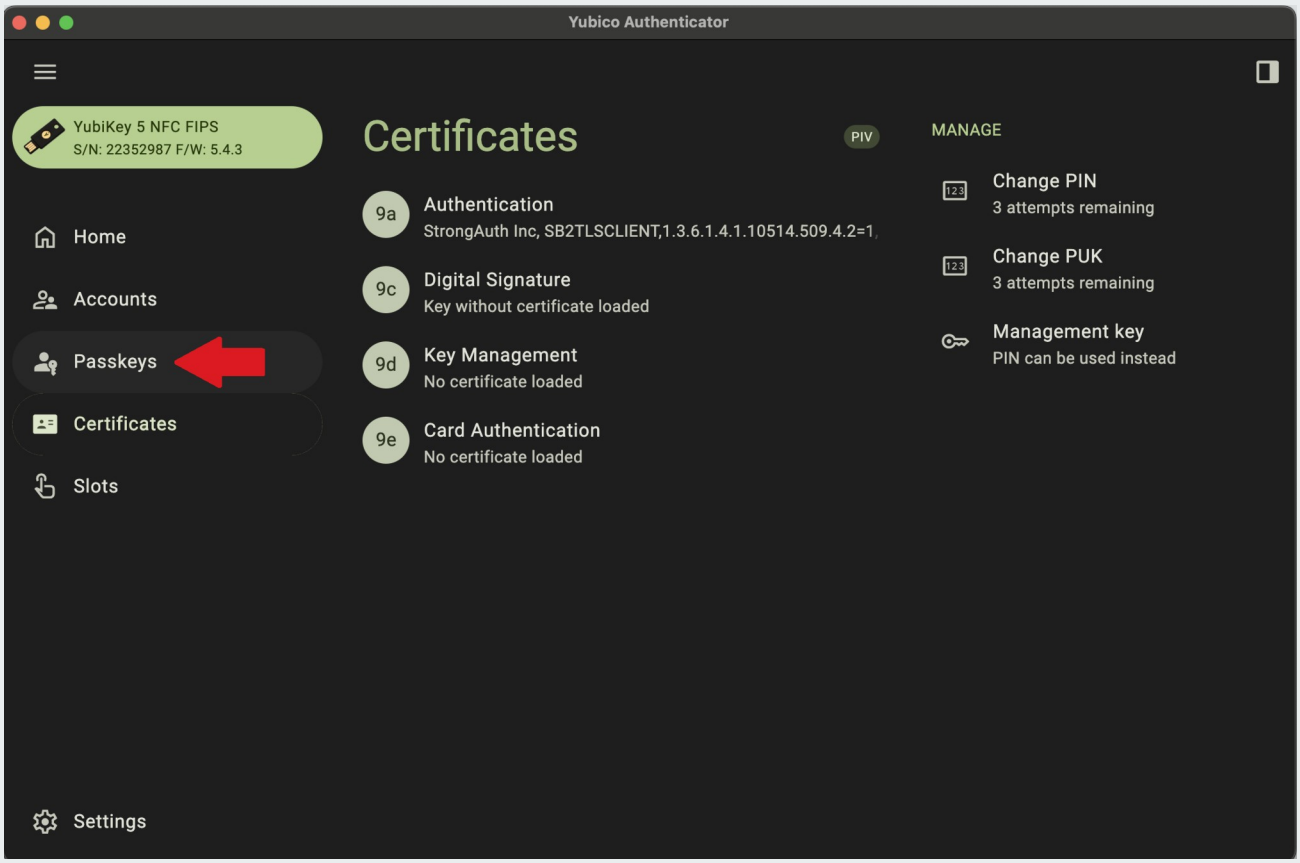
AP13 Save new PIN

Click Save. The application returns to the previous screen. If the process is successful, a **“PIN changed”** notification briefly appears at the bottom of the screen.



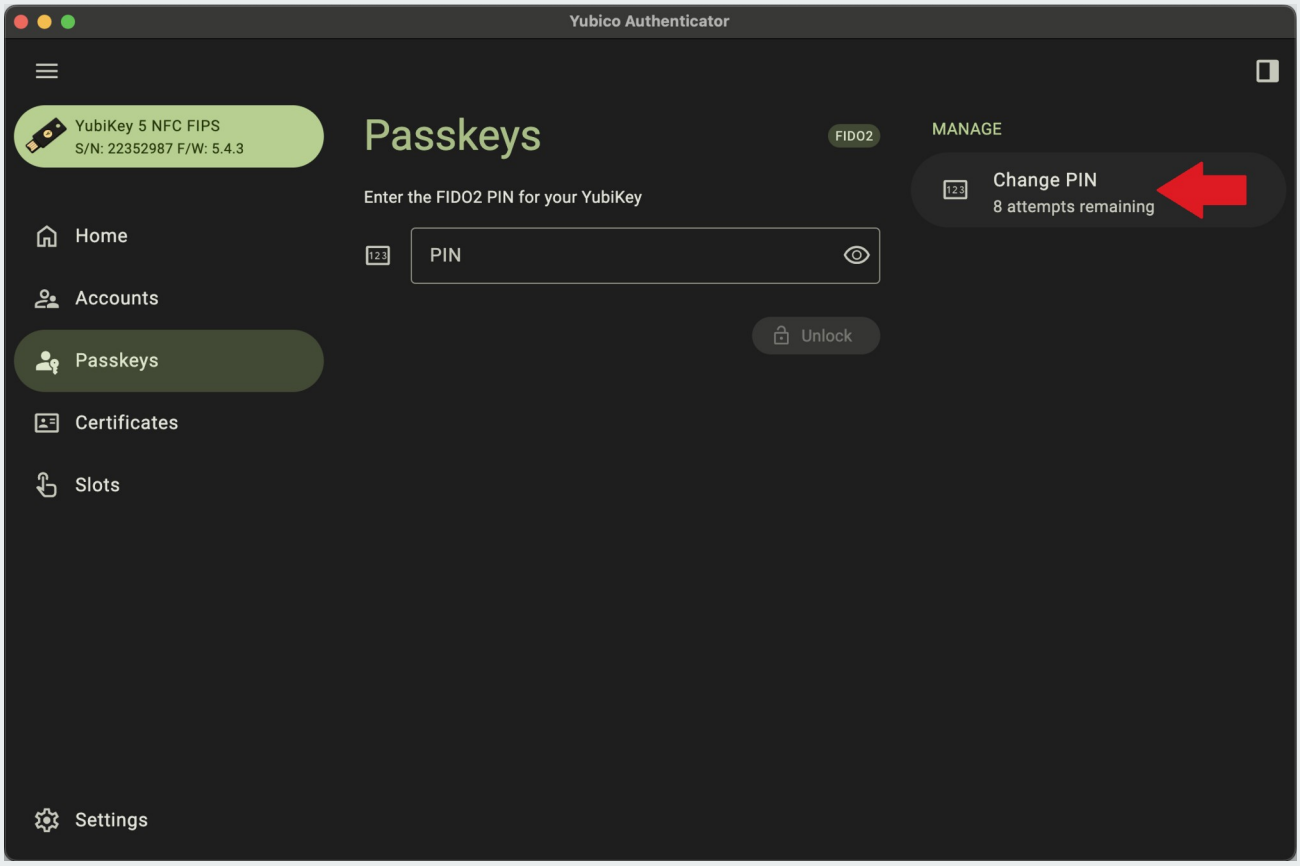
AP14 Changing the FIDO Credentials PIN

To update the second PIN, click on the **Passkeys** menu option to the left. **NOTE: StrongKey recommends using the same PIN for the Security Key.**



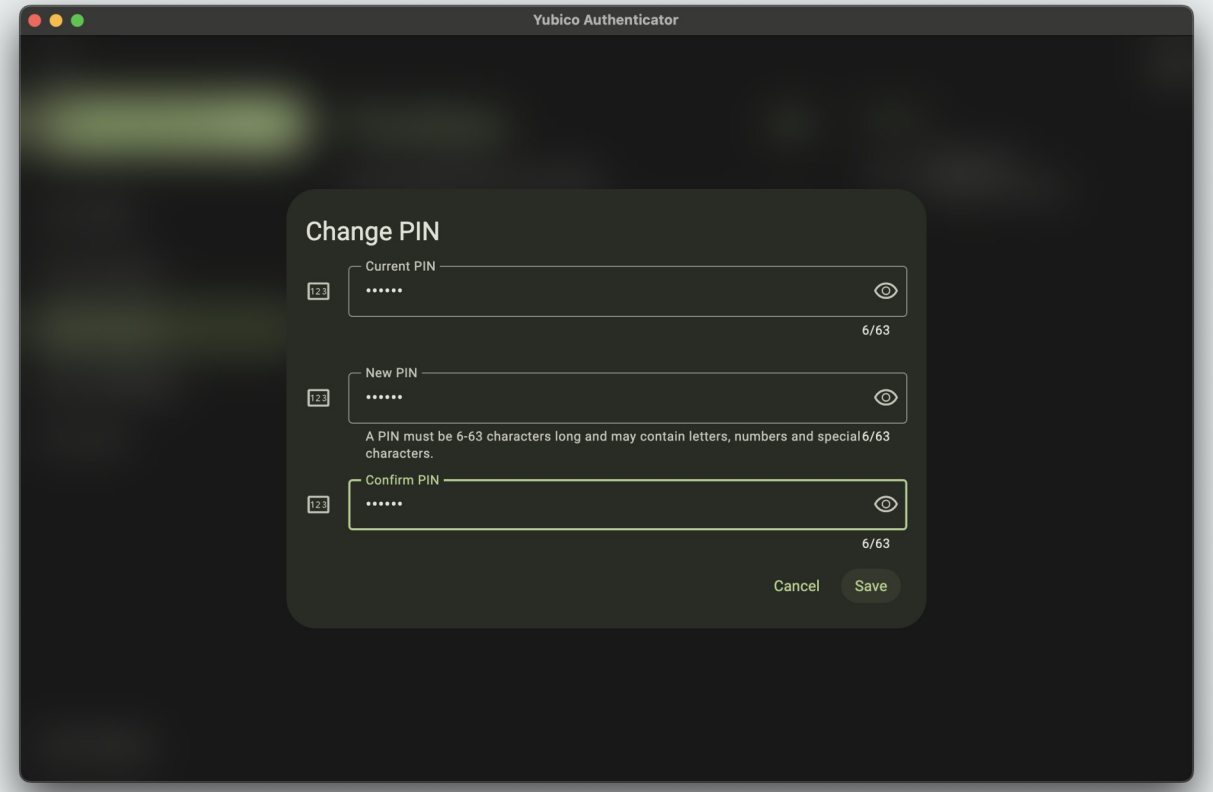
AP15 Change PIN option

Select the **Change PIN** option located on the right of the screen.



AP16 Enter PIN information

- In the text field marked **Current PIN,** type in your current PIN. If you have not changed it, it is 123456 by default.
- In the text field marked **New PIN** enter a new PIN of your choice. It must be a minimum of 6, and up to 63 characters.
- In the text field marked **Confirm PIN** enter the same PIN you selected.



AP19 Success!

The display will return to the **Passkeys** menu, and a notification stating "PIN Reset" will briefly appear at the bottom of the screen.