Smart Card on iOS

Yubico

Dec 06, 2022

CONTENTS

CHAPTER

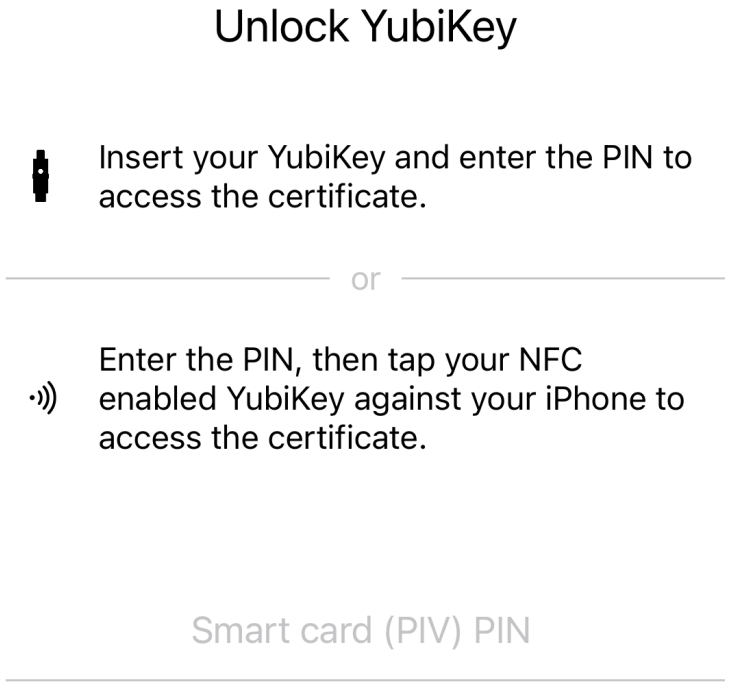
ONE

INTRODUCTION

The Smart Card on iOS feature within Yubico Authenticator facilitates smart card Transport Layer Security (TLS) authentication to websites from within the Safari browser. This feature is currently supported for iPhones/iPads with iOS/iPadOS 14.2 or later.

Smart Card on iOS allows you to easily provision the public portion of any smart card certificate stored on your YubiKey to the iOS Keychain on your iOS device. The private key of your smart card certificate remains on your YubiKey, from which it cannot be extracted.

During TLS authentication to a website, the public certificate is accessible to Safari via iOS Keychain, and Yubico Authenticator facilitates signing with the private key stored on your YubiKey. In order to complete authentication with Yubico Authenticator, you must plug your YubiKey into your iPhone/iPad (or scan if using an NFC-enabled YubiKey) and enter your smart card certificate PIN when prompted.



The Smart Card on iOS feature can also be used for signing emails and decrypting messages/documents. Please note that this guide focuses only on certificate-based authentication. Likewise, the feature also supports certificate-based authentication with third-party iOS applications, but the walkthrough included herein only covers the Safari browser usage.

1.1 X.509 Certificates

Both the iOS Keychain and the YubiKey can hold X.509 smart card certificates. Certificates are stored in the PIV application on the YubiKey, which contains 24 "slots" (for YubiKey 5 Series keys), four of which are easily accessible via the YubiKey Manager tool.

To enable the Smart Card on iOS functionality, both the public certificate and the private key need to be imported onto the YubiKey.

The YubiKey Manager tool supports importing of X.509 certificates and keys in the PEM, DER, and PKCS12 formats. For Smart Card on iOS, we recommend using certificates in the PKCS12 format (which have the .p12 and .pfx file extensions) as both the public certificate and private key are stored in the same file.

1.2 Prerequisites

To use the Smart Card on iOS feature, you must have the following:

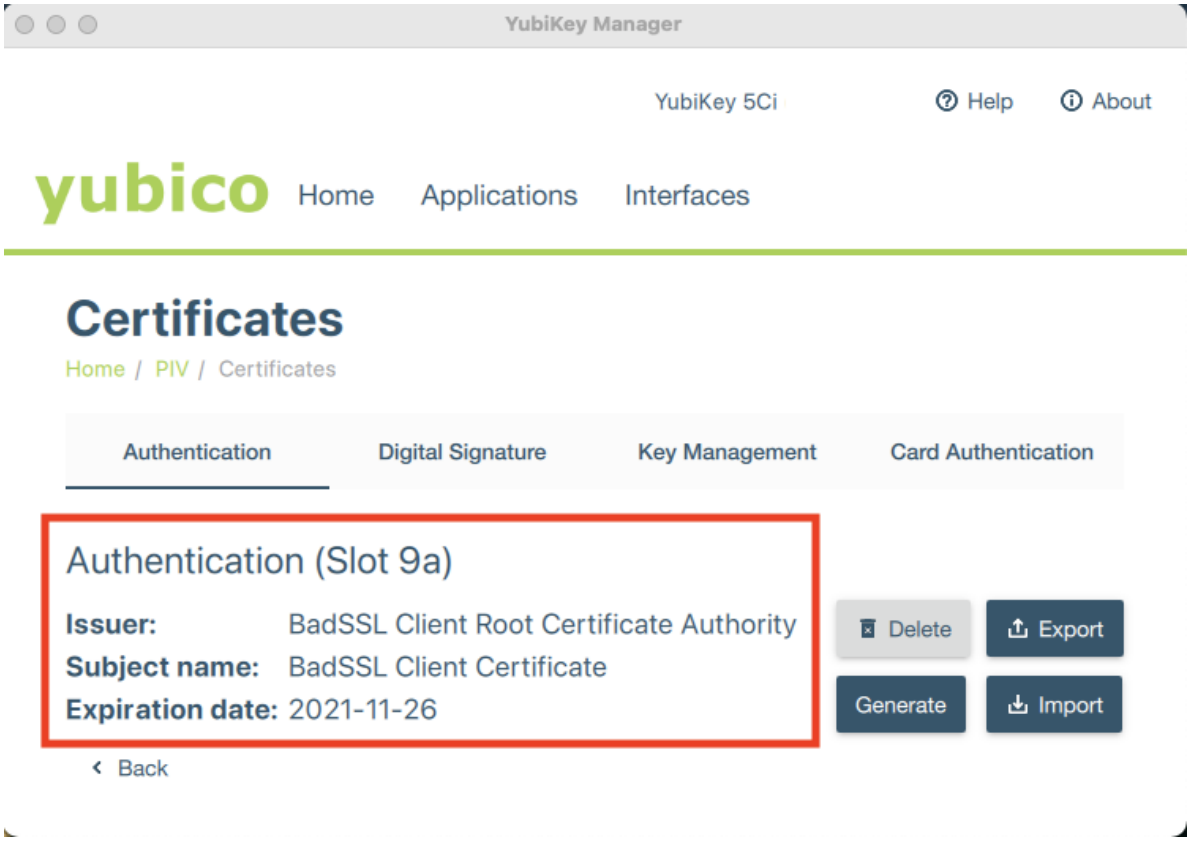
- Apple iPhone/iPad with iOS/iPadOS 14.2 or later.
- YubiKey 5 series key (5 NFC, 5C NFC, or 5Ci).
- Yubico Authenticator iOS application (v.1.6 or newer).
- Host computer.
- YubiKey Manager tool (available for Windows, Linux, and macOS).
- X.509 smart card certificate from a website you'd like to authenticate to. We recommend using the .p12 or .pfx file types if available. Download this file directly to your computer.

Note: If your YubiKey already has a smart card certificate stored in its PIV application, you only need an iPhone, your YubiKey, and Yubico Authenticator.

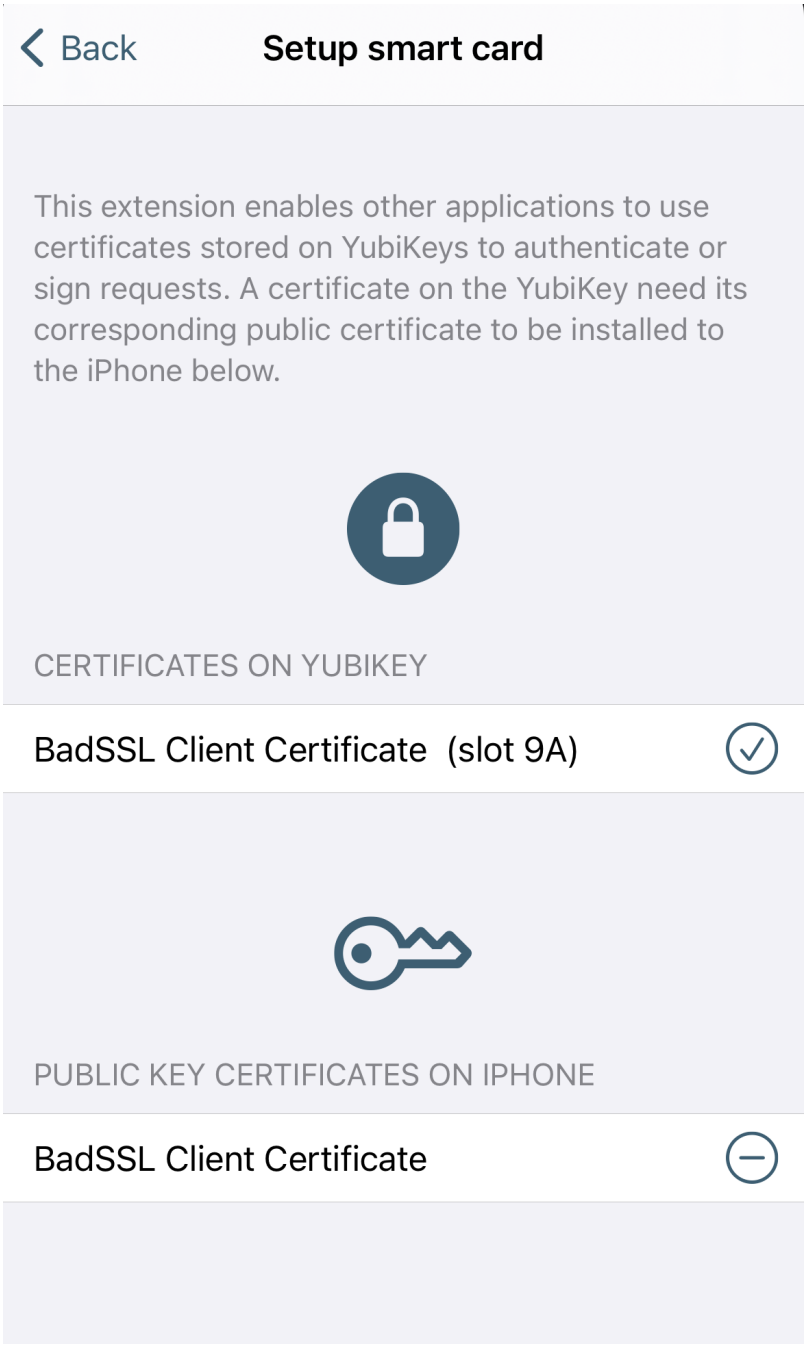
1.3 Overview: Setup Process

After satisfying the prerequisites listed above, do the following to set up and use the Smart Card on iOS feature (we use the BadSSL site for the example screenshots):

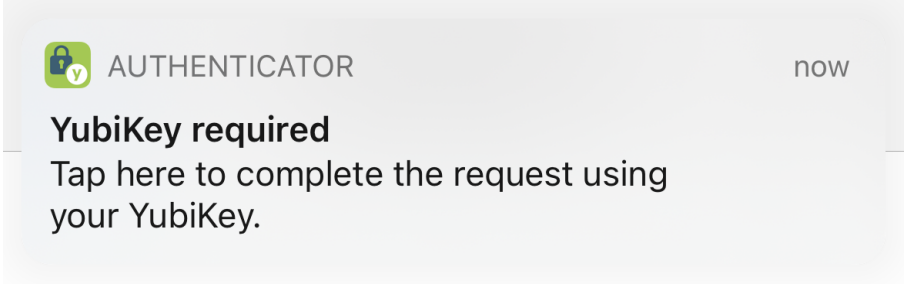
1. *Import your smart card certificate onto your YubiKey using YubiKey Manager.* If your YubiKey already has a certificate stored in its PIV application, skip to the next step.



2. *Provision the public certificate to your iOS Keychain* through the Yubico Authenticator application on your iOS device.



3. *Authenticate to the website that requires your smart card certificate on the Safari browser.*



1.4 Troubleshooting

If you run into issues using the Smart Card on iOS feature, check out the *Troubleshooting* chapter for possible solutions.

CHAPTER

TWO

IMPORT SMART CARD CERTIFICATES ONTO YOUR YUBIKEY

Before your smart card certificates can be provisioned to your iOS Keychain with Yubico Authenticator, you must first import those certificates onto a YubiKey from your host computer. This can be done through either of the following tools:

- YubiKey Manager GUI
- YubiKey Manager CLI

The GUI (graphical user interface) tool allows you to configure PIV functionality by clicking through a series of screens, whereas the CLI (command line interface) tool allows you to configure the same functionality through commands in a terminal. Both versions of the tool are supported for Windows, Linux, and macOS.

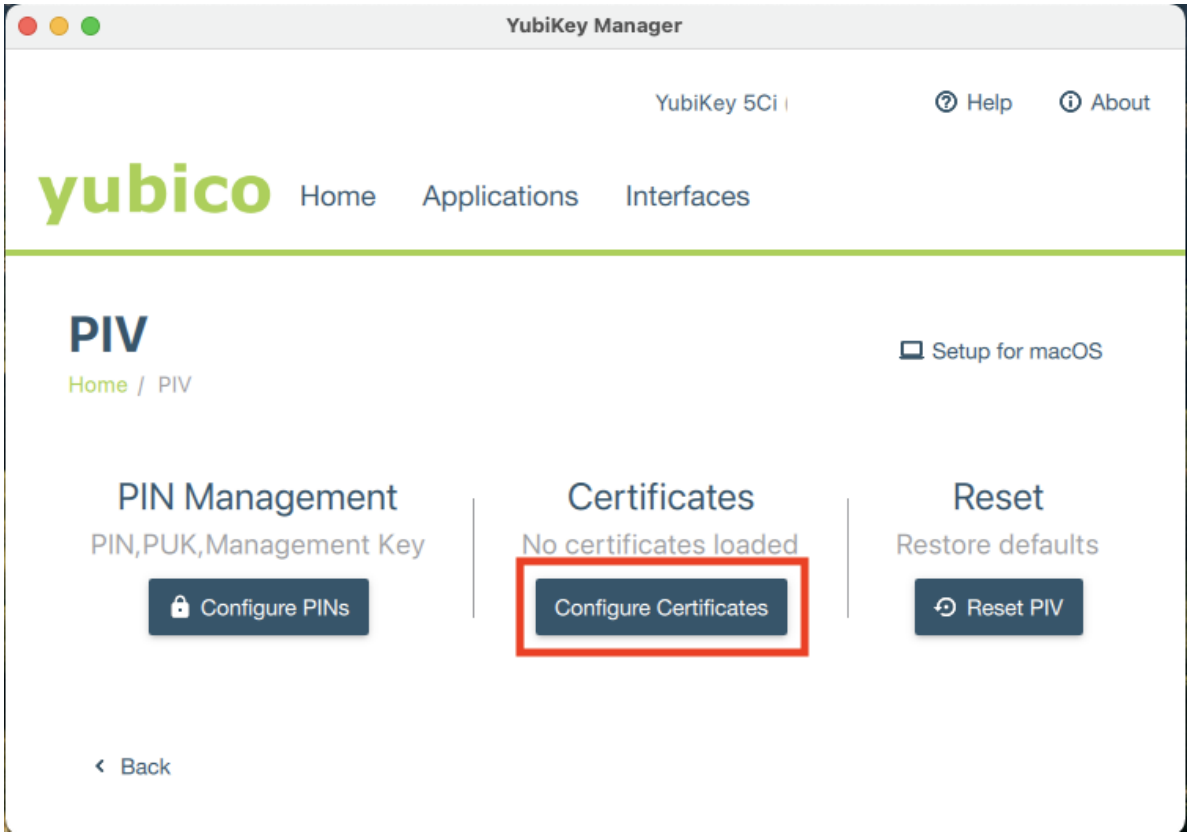
Follow the steps detailed below to import your smart card certificates onto your YubiKey using your preferred version of YubiKey Manager.

If you already have your smart card certificate stored on your YubiKey, skip to the next section: *Smart Card Certificate Provisioning with Yubico Authenticator*.

2.1 YubiKey Manager GUI

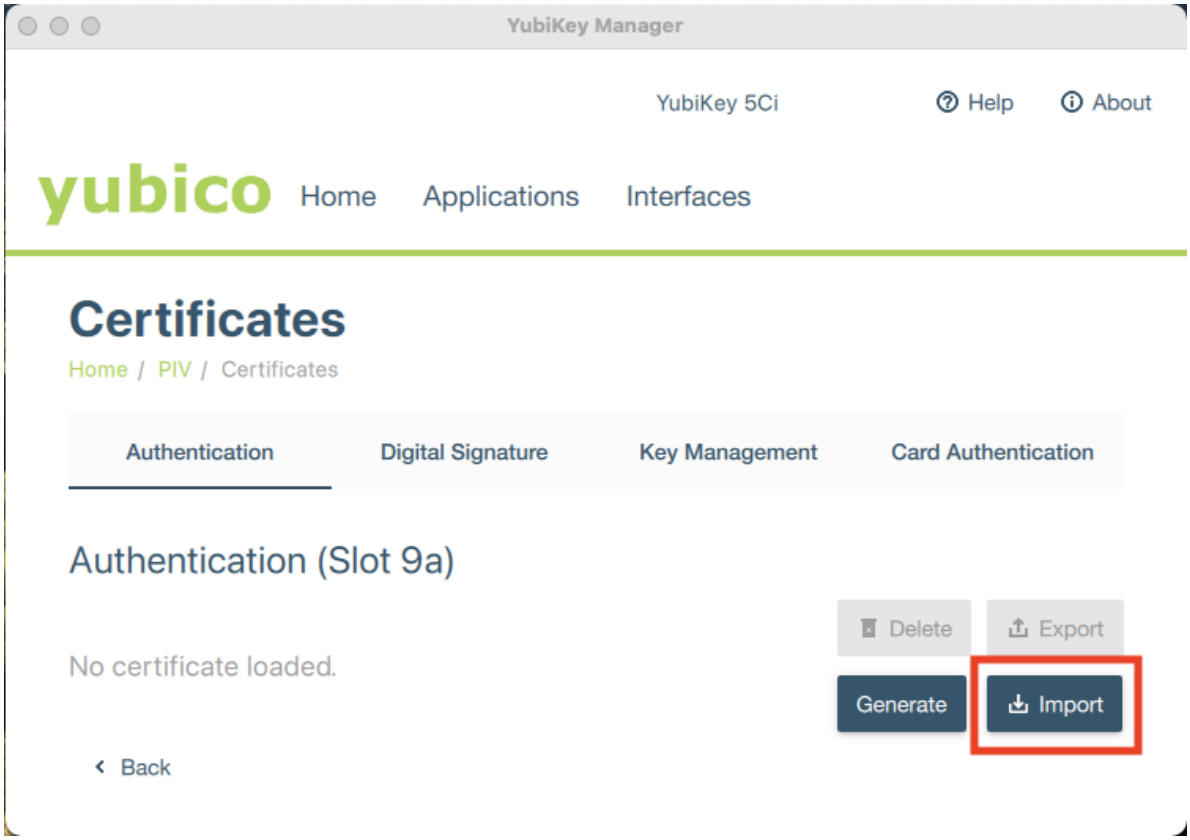
To use the GUI version of YubiKey Manager to import your certificate, follow the steps below:

1. If you haven't already, download the appropriate version of the YubiKey Manager GUI tool onto your host computer. Click on the downloaded file and follow the prompts to complete the installation.
2. Open the YubiKey Manager GUI tool and plug your YubiKey into your computer.
3. On the homepage of the YubiKey Manager, click on the **Applications** drop-down menu and select **PIV**.
4. Select **Configure Certificates** under the **Certificates** section.



5. The YubiKey has 24 total PIV slots, four of which are accessible via the YubiKey Manager tool (9a, 9c, 9d, and 9e). Technically, all of these accessible slots can be used to hold an X.509 certificate for authentication, but slot 9a is intended to be used for this purpose. For more information on PIV application slots, check out the slot documentation.

   Select an empty slot and click **Import**.



6. Navigate to the certificate file on your computer and select it to begin the import process.

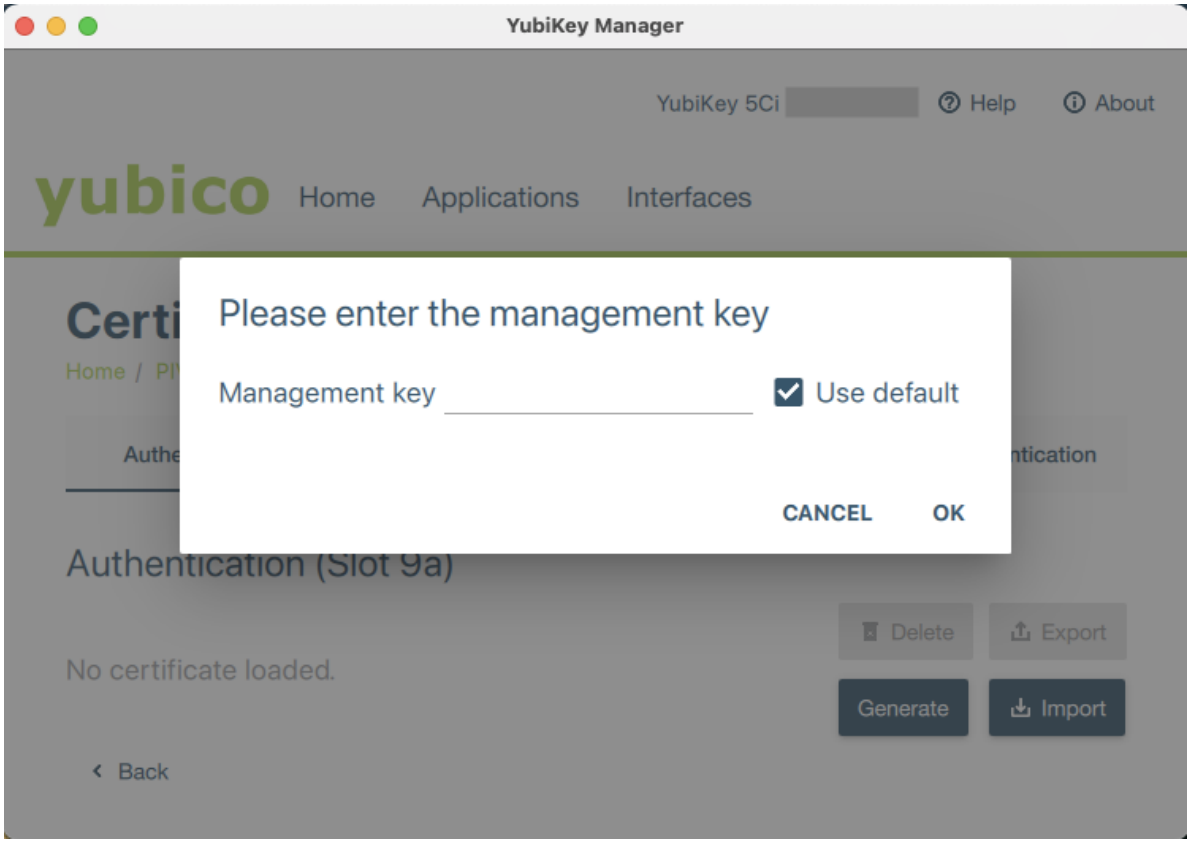
   Remember, the public certificate AND its private key must be imported onto your YubiKey. While the YubiKey can store any X.509 certificate of the PEM, DER, and PKCS12 format, we recommend using the PKCS12 file type (which have .pfx or .p12 file extensions) because the public certificate and private key are stored in a single file.

7. When prompted, enter the certificate's password and click **OK**.

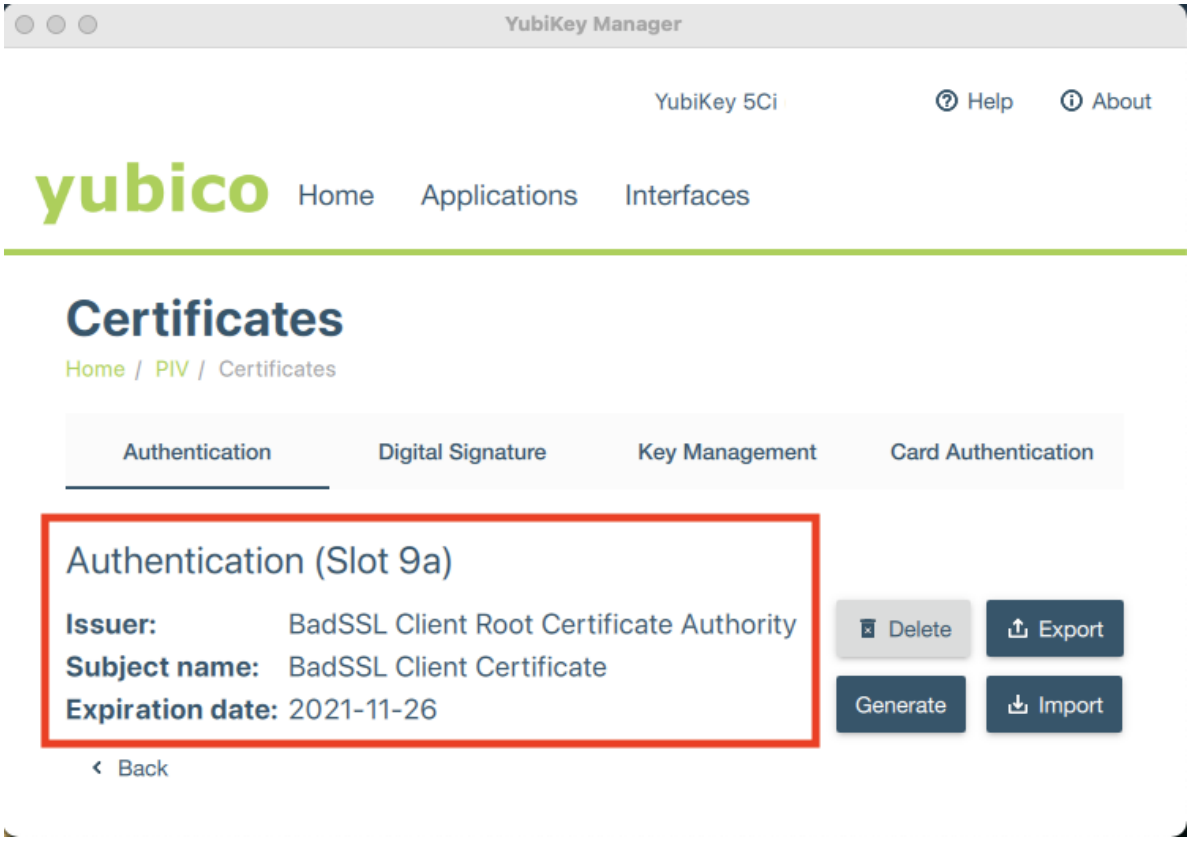
   Note: If you do not know your certificate's password, check with your admin (if applicable) or the certificate provider.

8. Next, enter the PIV application management key and click **OK**.

   Note: If you have not changed the management key using YubiKey Manager, the default managment key will be sufficient. If your YubiKey is managed by your organization, reach out to your admin for your management key.



9. If the import was successful, the slot will display the issuer, subject name, and expiration date of the imported certificate.



10. Repeat this process to import additional smart card certificates as needed.

2.2 YubiKey Manager CLI

If you prefer to use the command line version of the YubiKey Manager tool (ykman) to import your certificate, follow the steps below:

1. Install ykman onto your host computer.
2. ykman can be run within a command prompt, terminal, or PowerShell. Please see the ykman documentation for more information on configuring your system to do this.
3. Once your system has been configured, open a command prompt, terminal, or PowerShell.
4. Plug your YubiKey into your computer.
5. The YubiKey has 24 total PIV slots, four of which are accessible via the YubiKey Manager tool (9a, 9c, 9d, and 9e). Technically, all of these accessible slots can be used to hold an X.509 certificate for authentication, but slot 9a is intended to be used for this purpose. For more information on PIV application slots, check out the slot documentation.

   Enter `ykman piv info` to check if any slots on your YubiKey are already occupied.
6. Once you have identified an appropriate empty slot, navigate to the folder containing your smart card certificate.
7. Enter `ykman piv certificates import <slot> <filename>` to import your certificate onto your YubiKey. `<slot>` refers to the slot number (e.g. 9a), and `<filename>` refers to the name of your certificate file (e.g. certificate.p12).

Remember, the public certificate AND its private key must be imported onto your YubiKey. While the YubiKey can store any X.509 certificate of the PEM, DER, and PKCS12 format, we recommend using the PKCS12 file type (which have .pfx or .p12 file extensions) because the public certificate and private key are stored in a single file.

8. When prompted, enter your certificate's password and your PIV application management key.

Note: If you do not know your certificate's password, check with your admin (if applicable) or the certificate provider. If you have not changed the management key using YubiKey Manager, the default managment key will be sufficient. If your YubiKey is managed by your organization, reach out to your admin for your management key.

---

9. Enter `ykman piv info` again to verify that the certificate import was successful. You will see the slot number listed along with the certificate algorithm, subject DN, issuer DN, serial number, fingerprint, and the time period the certificate is valid for.

Note: For more information on ykman PIV commands, please see the ykman documentation.

```
ML-EQUIJANO-01:~ e.quijano$ cd Downloads/
ML-EQUIJANO-01:Downloads e.quijano$ ykman piv certificates import 9a badssl.com-client.p12
Enter password to decrypt certificate:
Enter a management key [blank to use default key]:
ML-EQUIJANO-01:Downloads e.quijano$ ykman piv info
PIV version: 5.2.7
PIN tries remaining: 3
Management key algorithm: TDES
CHUID:

CCC:    No data available.
Slot 9a:
        Algorithm:      RSA2048
        Subject DN:     CN=BadSSL Client Certificate,O=BadSSL,L=San Francisco,ST=California,C=US
        Issuer DN:      CN=BadSSL Client Root Certificate Authority,O=BadSSL,L=San Francisco,ST=California,C=US
        Serial:
        Fingerprint:
        Not before:     2019-11-27 00:19:57
        Not after:      2021-11-26 00:19:57
ML-EQUIJANO-01:Downloads e.quijano$
```

10. Repeat this process to import additional smart card certificates as needed.

2.3 Next Steps

Now that you have imported your smart card certificate onto your YubiKey, you may *provision the certificate to your iOS Keychain* through the Yubico Authenticator application on your iOS device.

CHAPTER

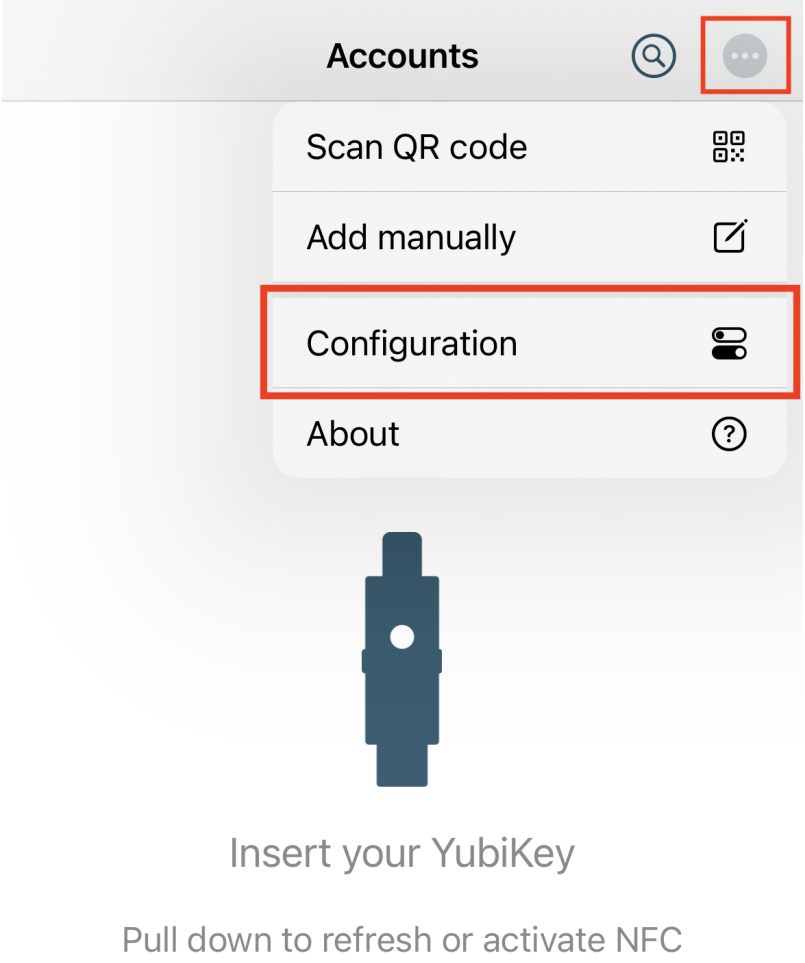
THREE

SMART CARD CERTIFICATE PROVISIONING WITH YUBICO AUTHENTICATOR

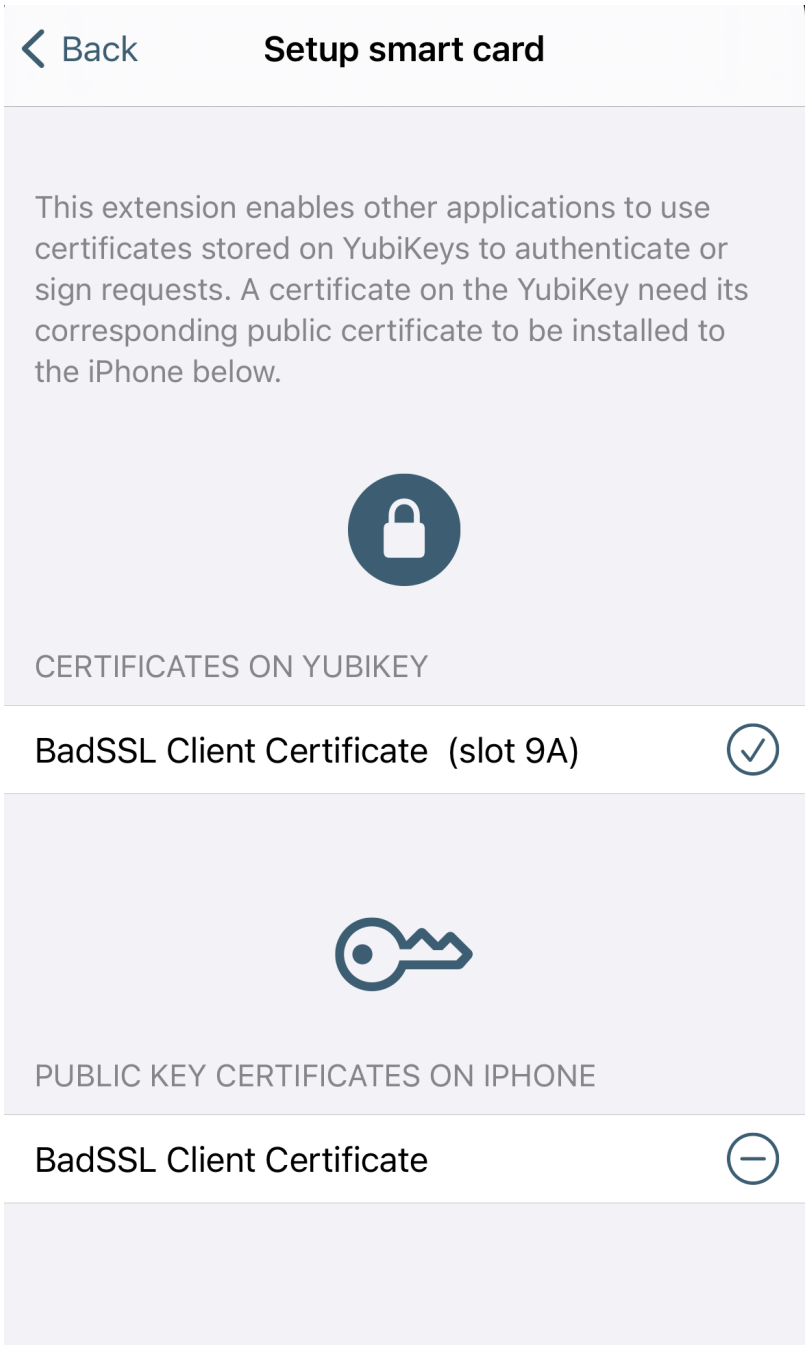
Now that your smart card certificates have been *imported onto your YubiKey*, you must provision the public portion of the certificates onto your iOS Keychain through Yubico Authenticator. After completing this step, you will be able to use the Smart Card on iOS feature to autheticate to the websites that require those smart card certificates on the Safari browser.

3.1 Provision Your Public Certificate

1. If you haven't already, download and install the Yubico Authenticator application (v.1.6 or newer) onto your iOS device.
2. Open Yubico Authenticator.
3. On the home screen of Yubico Authenticator, click on the three dots (...) in the upper right corner of the screen and select **Configuration**.



4. On the **Configuration** screen, select **Setup smart card (PIV)**.
5. Insert your YubiKey into your device. If you are using a YubiKey with NFC capabilities, scan your key.
6. Once your YubiKey has been detected by the app, all certificates stored on your YubiKey will appear under **CERTIFICATES ON YUBIKEY**. To provision the public certificate from one of your PIV application slots to your iOS Keychain, click the appropriate (**+**) icon.
7. If the provisioning was successful, the name of your certificate will appear under **PUBLIC KEY CERTIFICATES ON IPHONE**. You may remove certificates from your iOS Keychain at any time by clicking the (**–**) icon next to the certificate name.



3.2 Next Steps

Congratulations! Your public certificate has been provisioned to your iOS device, and you are now ready to authenticate to the website requiring that smart card certificate on Safari. See *Authenticating with Smart Card on iOS* for guidance.

CHAPTER

FOUR

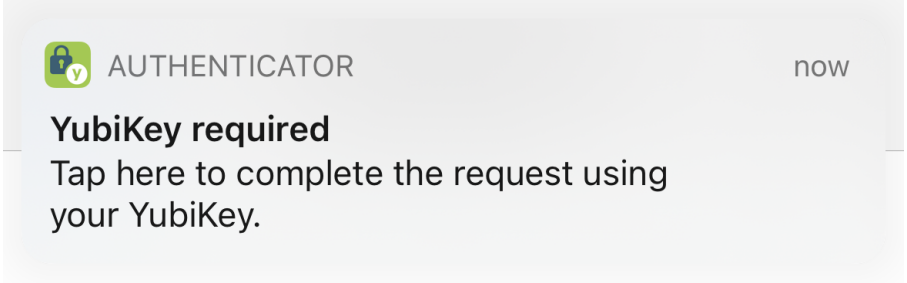
AUTHENTICATING WITH SMART CARD ON IOS

Now that you have *imported your smart card certificates onto your YubiKey* and *provisioned the public portions of the certificates to your iOS Keychain* through Yubico Authenticator, you are ready to use the Smart Card on iOS feature to authenticate to the websites corresponding to your provisioned certificates on Safari.

Follow the steps below for guidance on how to use the Smart Card on iOS feature.

4.1 Authenticate to a Website on Safari

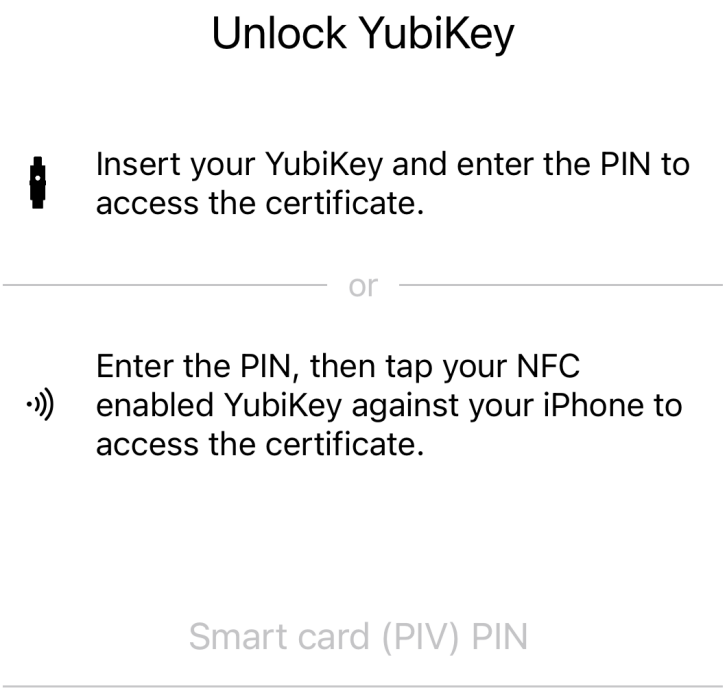
1. Click the compass icon to open the Safari browser on your iOS device.
2. Enter the URL of the website you'd like to authenticate to. The website must correspond to a public certificate stored in your iOS Keychain.
3. If you have more than one certificate stored in your iOS Keychain, or if you are browsing in private mode on Safari, you will be asked to confirm which certificate you'd like to use for authentication. Follow the prompts as necessary.
4. A pop-up from Yubico Authenticator will appear at the top of the screen. Click on the pop-up to begin the authentication.



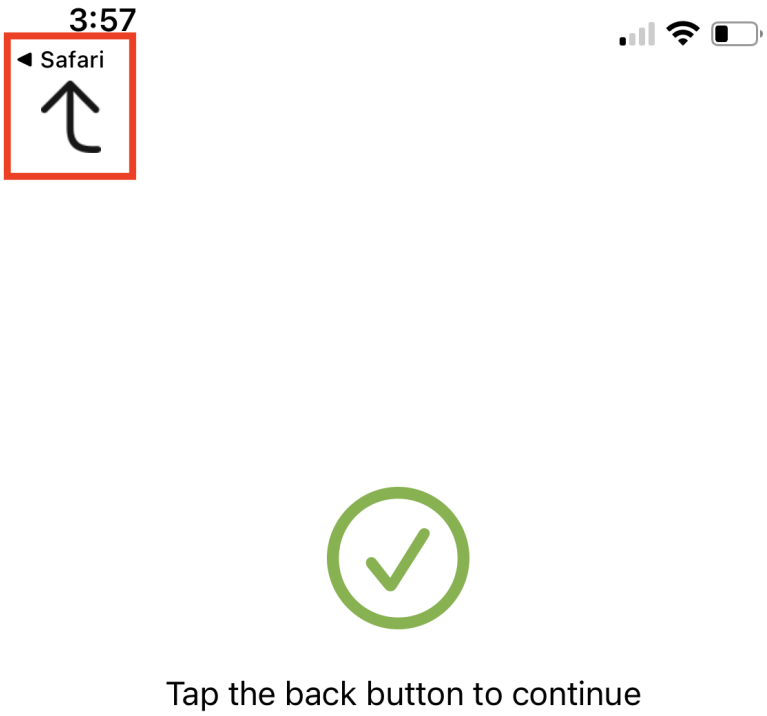
5. Insert your YubiKey into your iOS device, and type in your PIV application pin. If you are using an NFC-enabled YubiKey, enter your PIN first and then tap your key to scan.

   The default PIV application PIN is 123456. If you reset your PIN using YubiKey Manager, enter that number here. If your YubiKey is managed by your organization, reach out to your admin for your PIN.

> **Caution:** You only have three attempts to enter the correct PIN before your YubiKey is locked.



6. If you entered the correct PIN and authentication was successful, you will see a green check mark. Click on **Safari** in the upper left corner to return to your browser.



7. After returning to Safari, you will be logged into the website.

CHAPTER

FIVE

TROUBLESHOOTING

Running into issues using the Smart Card on iOS feature? Check the guidance below for possible solutions.

5.1 Web Browser Does Not Trigger the Yubico Authenticator Application

Problem: when trying to authenticate to a website, the browser does not trigger the Yubico Authenticator application, and the pop-up that allows you to complete your authentication request does not appear. You may have received a timeout error or a message about an inability to create a secure connection.

Solution: iOS Focus modes, such as Do Not Disturb, Sleep, Personal, and Work, suppress notifications, including the Yubico Authenticator pop-up. If you have a Focus mode turned on, you will see the mode's symbol on your lock screen (e.g. Do Not Disturb uses a moon symbol). To use the Smart Card on iOS feature with Yubico Authenticator, you must turn off all focus modes *or* add Yubico Authenticator as an Allowed Notification for each mode.

5.1.1 Toggle Focus Modes Off

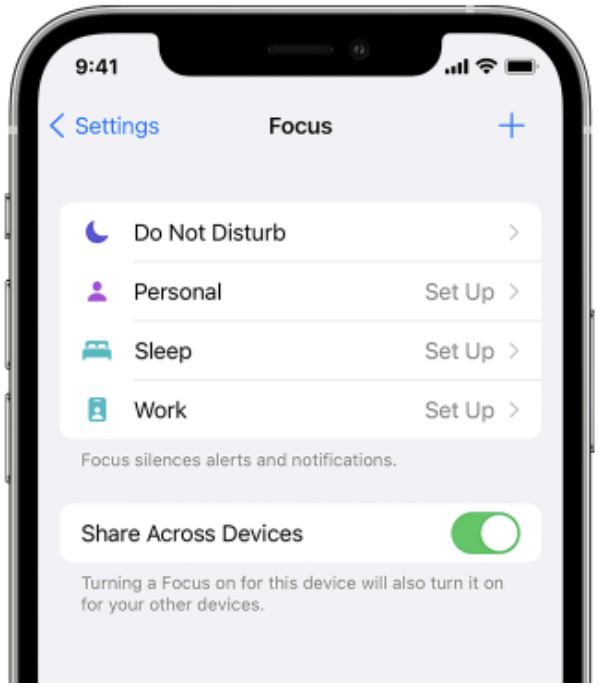
To toggle your Focus modes off, do the following:

1. Open your Control Center.
2. Select the Focus icon and toggle all modes to the off position.

5.1.2 Add Yubico Authenticator as an Allowed Notification

If your device is running iOS/iPadOS 15 or higher, and you would like to keep your Focus modes on while using the Smart Card on iOS feature, you may instead add Yubico Authenticator as an Allowed Notification.

1. Go to **Settings** > **Focus**.
2. Click on each Focus mode (Do Not Disturb, Personal, Sleep, and Work), select **Allowed Notifications**, and choose the Yubico Authenticator application.


9:41
Settings
Focus
Do Not Disturb
Personal
Set Up
Sleep
Set Up
Work
Set Up
Focus silences alerts and notifications.
Share Across Devices
Turning a Focus on for this device will also turn it on for your other devices.

CHAPTER

SIX

COPYRIGHT

6.1 Trademarks

Yubico and YubiKey are registered trademarks of Yubico AB. All other trademarks are the property of their respective owners; in particular, Apple, Lightning®, Mac, and MacOS are trademarks of Apple Inc., registered in the U.S. and other countries.

6.1.1 Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design, and manufacturing. Yubico shall have no liability for any error or damages of any kind resulting from the use of this document.

The Yubico Software referenced in this document is licensed to you under the terms and conditions accompanying the software or as otherwise agreed between you or the company that you are representing.

6.1.2 Contact Information

Yubico Inc.
5201 Great America Parkway
#122
Santa Clara, CA 95054
USA

To get in touch with Yubico Support, click here. More options for getting touch with us are available on the Contact page of Yubico's website.

6.1.3 Document Updated

2022-12-06 00:12:55 UTC