

UNCLASSIFIED

UNITED STATES DEPARTMENT OF STATE



PUBLIC KEY INFRASTRUCTURE (PKI) PROGRAM OFFICE MAC LAPTOP CERTIFICATE UPDATE PROCEDURES

VERSION 1.0

February 2024

UNCLASSIFIED

UNCLASSIFIED

DOCUMENT VERSION CONTROL

Version	Date	Author(s)	Description	Reason for Change
1.0	February 2024	A. Beard	Initial Draft	Initial publication

UNCLASSIFIED

UNCLASSIFIED

TABLE OF CONTENTS

1. INTRODUCTION.....	1
1.1. SCOPE	1
1.2. AUDIENCE.....	1
2. INSTALLING DOS ROOT CERTIFICATES.....	2
2.1. PROCEDURES.....	2
3. CONNECTING A SMARTCARD TO A MAC	7
3.1. REFERENCE MATERIAL	8

TABLE OF TABLES

TABLE 2-1, CERTIFICATE INSTALLATION	2
TABLE 3-1, SMARTCARD SETUP	7

UNCLASSIFIED

UNCLASSIFIED

FEDERAL APPROVAL

The following signature validates that this document is approved by the federal government.

Paul J Newton

Digitally signed by Paul J Newton
Date: 2024.04.02 14:11:38
-04'00'

Paul Newton

PKI Program Manager

IRM/FO/ITI/SI/IIB/PKI Program Office

UNCLASSIFIED

UNCLASSIFIED

1. INTRODUCTION

This document addresses the proper procedure for updating laptops running the MAC operating system with Department of State (DOS) certificates. The actions are provided as a reference for end users to ensure they know the procedures for this process.

1.1. SCOPE

This document will provide the end user with the steps to install the DOS Root certificates to enable trust with DOS systems resulting in smartcard login, using Personal Identity Verification (PIV) smartcards, on MAC OS Monterrey, Ventura and Sonoma.

1.2. AUDIENCE

This document is intended for DOS employees who use MAC operating system laptops to log into the Department's unclassified network.

UNCLASSIFIED

UNCLASSIFIED

2. INSTALLING DOS ROOT CERTIFICATES

2.1. PROCEDURES

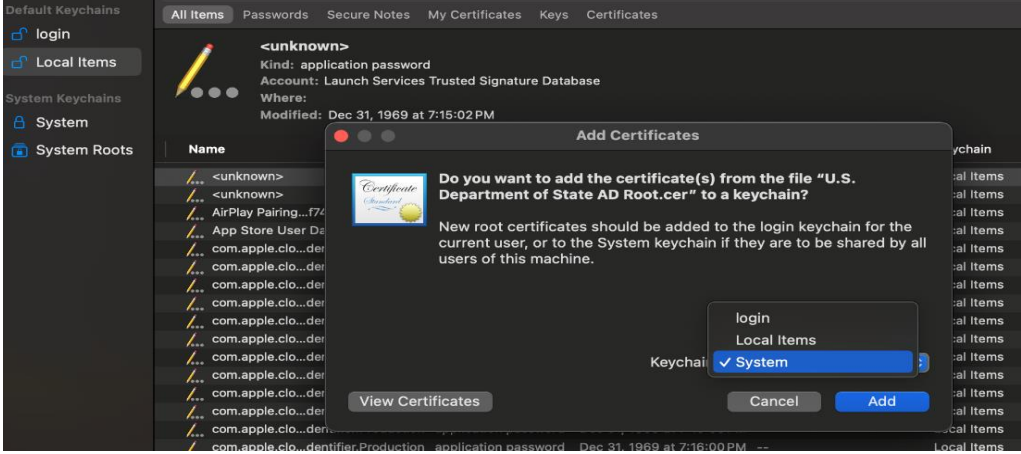
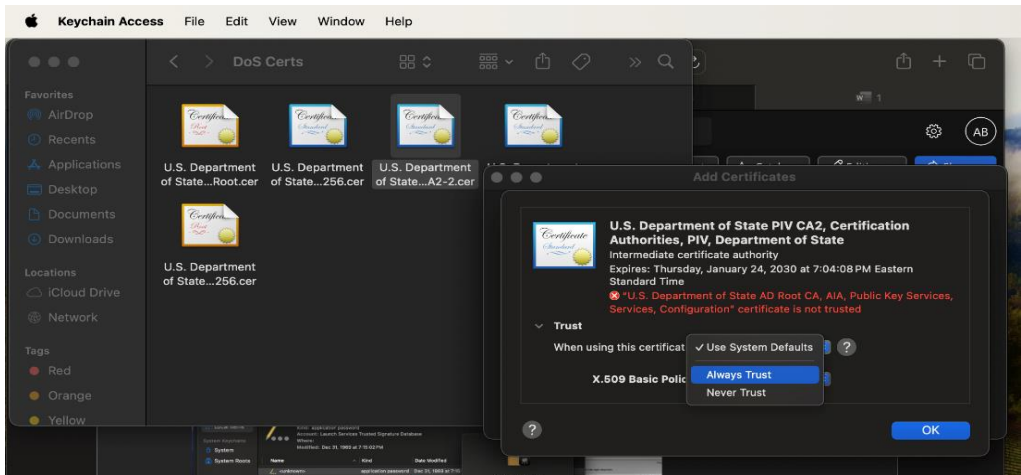
Table 2-1, Certificate Installation

Step	Action
1.	Download “DoS Certs.zip” file from the PIV Software download section on the site https://pkaps.pki.state.gov/WebCardTest/ -In the Download folder on the MAC click on the DoS Certs folder. 
2.	The following steps will be repeated for all 5 of the certificates in the DoS Certs folder.

UNCLASSIFIED

UNCLASSIFIED

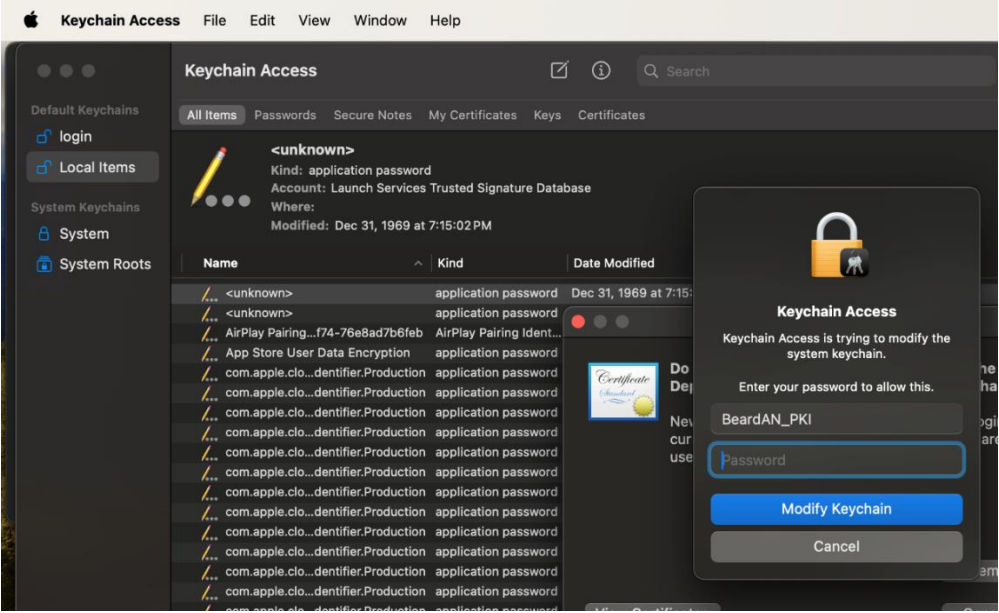
Table 2-1, Certificate Installation

Step	Action
3.	Double click on each certificate. The Keychain Access manager window will appear in the background with a smaller window labeled ‘Add Certificates’ in the front. Select System in the drop-down menu then select “View Certificate” 
4.	Select “Trust”. In the drop-down, change System Defaults to “Always Trust”. Click “OK” then the “Add” button. 

UNCLASSIFIED

UNCLASSIFIED

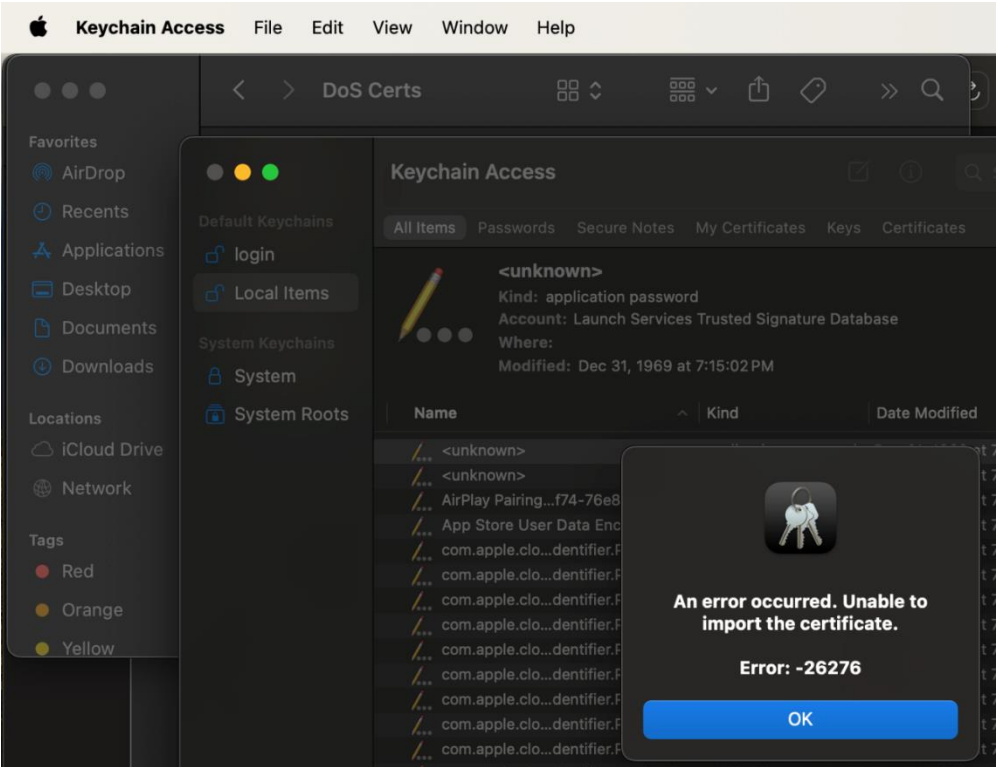
Table 2-1, Certificate Installation

Step	Action
5.	Enter your MAC Computer Login to confirm the Keychain Modification.  The screenshot shows the Keychain Access application window. The left sidebar lists 'Default Keychains' (login, Local Items) and 'System Keychains' (System, System Roots). The main pane shows a list of items under the 'All Items' tab. The first item is '<unknown>' with a pencil icon, 'Kind: application password', 'Account: Launch Services Trusted Signature Database', and 'Where:'. Below this is a table with columns 'Name', 'Kind', and 'Date Modified'. The table lists several items, including '<unknown>', 'AirPlay Pairing...', 'App Store User Data Encryption', and multiple entries for 'com.apple.clo...identifier.Production'. A 'Certificate' dialog box is visible in the background. In the foreground, a 'Keychain Access' password prompt dialog is open, asking for a password to allow the modification of the system keychain. The dialog shows the username 'BeardAN_PKI' and a 'Password' field. The 'Modify Keychain' button is highlighted in blue.

UNCLASSIFIED

UNCLASSIFIED

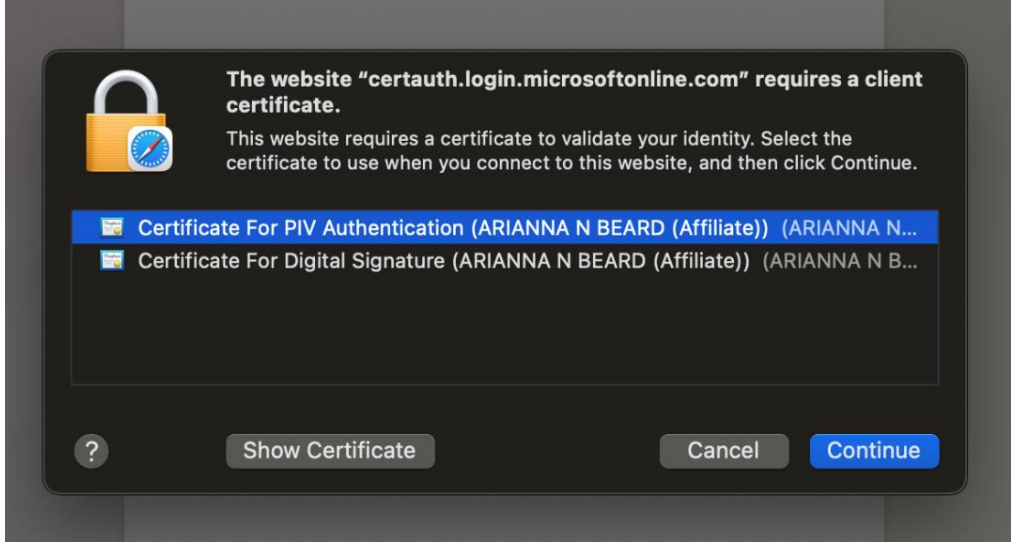
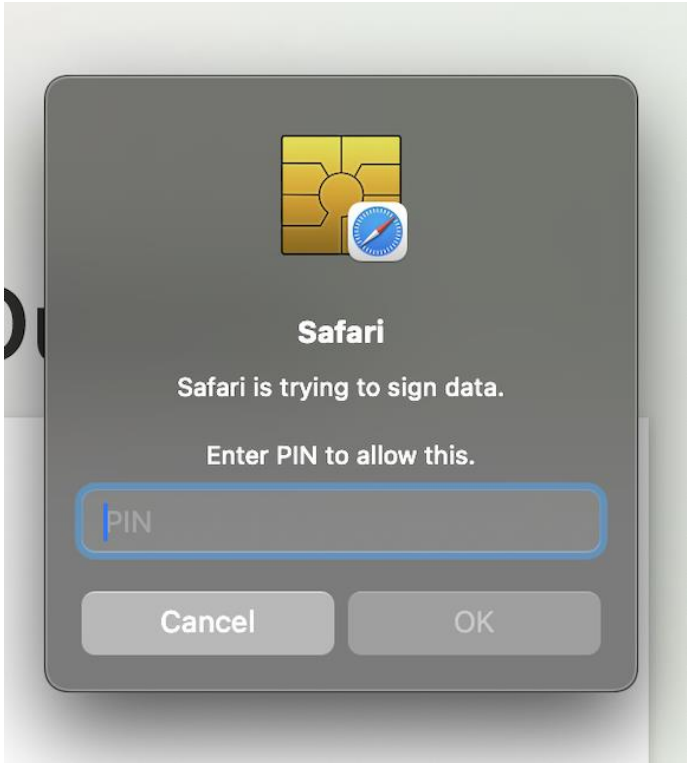
Table 2-1, Certificate Installation

Step	Action
6.	For error message -26276, please select “OK” and continue with the next certificate. NOTE: This certificate is still in the computer that will allow you to access DoS sites. 
7.	Navigate to GO Browser or GO Virtual once the certificates have been imported.

UNCLASSIFIED

UNCLASSIFIED

Table 2-1, Certificate Installation

Step	Action
8.	When prompted, choose the <i>Certificate for PIV Authentication</i> 
9.	Input Enter your 6-digit PIN associated with your smart card. Select “OK” button. 

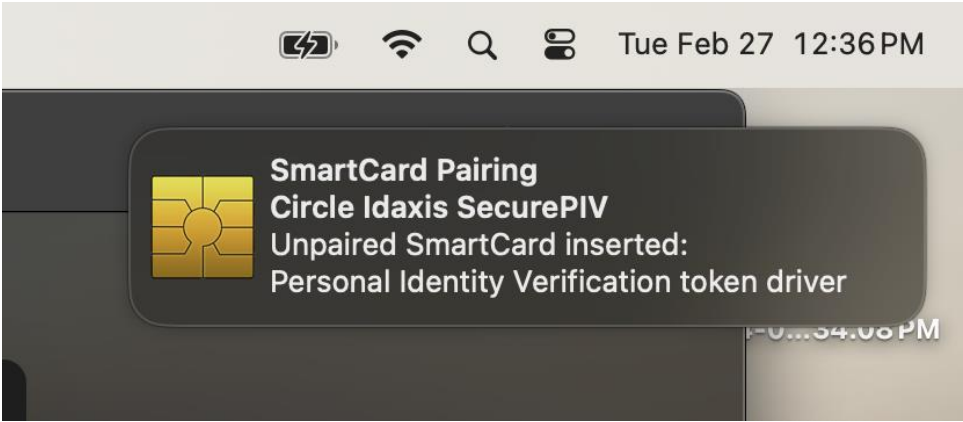
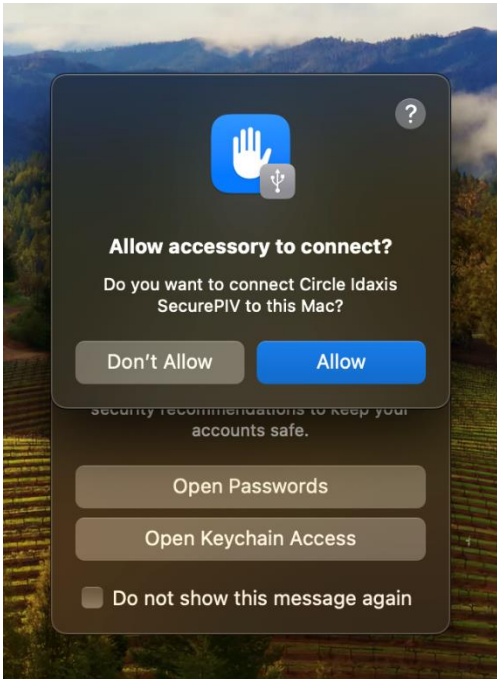
UNCLASSIFIED

UNCLASSIFIED

3. CONNECTING A SMARTCARD TO A MAC

This section will provide the end user with procedures to connect their smartcard to their MAC device. When logging back into your MAC, ensure that you are **NOT PAIRING** your PIV Smartcard and **ALLOW** your card to connect to your MAC.

Table 3-1, Smartcard Setup

Step	Action
1.	Launch Do not PAIR. Exit out of this notification.  A screenshot of a macOS notification. At the top, the status bar shows battery, Wi-Fi, search, and a smartcard icon, along with the date and time 'Tue Feb 27 12:36 PM'. The notification itself has a dark background and features a yellow smartcard icon on the left. The text reads: 'SmartCard Pairing', 'Circle Idaxis SecurePIV', 'Unpaired SmartCard inserted:', and 'Personal Identity Verification token driver'. A timestamp 'Feb 27 12:34:08 PM' is visible in the bottom right corner of the notification.
2.	Click on “Allow” to connect your card reader to the MAC  A screenshot of a macOS system dialog box titled 'Allow accessory to connect?'. It features a blue icon of a hand with a USB symbol. The text asks: 'Do you want to connect Circle Idaxis SecurePIV to this Mac?'. There are two buttons: 'Don't Allow' (grey) and 'Allow' (blue). Below the buttons, there is a link to 'security recommendations to keep your accounts safe.' and two more buttons: 'Open Passwords' and 'Open Keychain Access'. At the bottom, there is a checkbox labeled 'Do not show this message again'.

UNCLASSIFIED

UNCLASSIFIED**3.1. REFERENCE MATERIAL**

For additional information on pairing your PIV badge to your MAC, please reference “Setting up a MAC for accessing DOS resources with a PIV Card reader” via

<https://docs.google.com/document/d/1e7wBRQragEGo3NT0aKWbS6FPo9H2geeAN2ADidE9WGE/edit#heading=h.zi8e2objsplh>

UNCLASSIFIED