Homeland Security

DHS Federal Network Resilience

Federal PKI Trust Removal from Apple Certificate Stores

August 02, 2018

Federal Network Resilience Division
Office of Cybersecurity and Communications
National Protection and Programs Directorate

Agenda

Welcome

- Branko Bokan, DHS/FNR

Background

- General Services Administration

U.S. Government Root Certificate Removal

- General Services Administration

Questions and Open Discussion

- All participants

Welcome

Call Reminders

- **Phones**: All participants will be muted during the first part of the webinar. We will open the lines for the Q&A session. Please mute your phone if you are not speaking.

  Do not place the call “On Hold.”

- **Discussion:** We will have Q&A at the end of the call.

- **Roll Call**: Using the Adobe Connect poll feature, provide your full name, email address, and your full agency name/component.

- **Participation**: We encourage active participation from agency callers. Please use the Adobe Connect session to ask questions or comment throughout the session.

About

- The Federal Public Key Infrastructure (PKI) root Certification Authority (CA) certificate will be removed from commercial certificate stores

- The change will impact all federal agencies across multiple services

- GSA, in coordination with DHS, supporting remediation efforts

Microsoft Certificate Store

- The Federal Public Key Infrastructure (PKI) root Certification Authority (CA) certificate will be removed from Microsoft's certificate store in 2019

- Target date for remediation December 31, 2018

Apple Certificate Stores

- The Federal Public Key Infrastructure (PKI) root Certification Authority (CA) certificate will be removed from Apple certificate stores in the release of macOS Mojave and iOS 12 (estimated release September to October 2018)
- This change will not affect macOS 10.13 and below or iOS 11 and below
- Target date for remediation August 31, 2018

Listserv

To receive updates on the removal of the Federal PKI root certificate from commercial certificate stores you can subscribe to a mailing list created for this purpose.

Send an email with your full name, agency, and sub-agency/component name to:

fpkitruststoreremoval@gsa.gov

Web Repository

Details and relevant information on the removal of Federal PKI trust from the Apple certificate stores will be maintained here:

https://fpki.idmanagement.gov/truststores/apple/

Contacts

For technical inquiries and recommended actions, please contact GSA teams at:

fpki@gsa.gov

For general inquiries on DHS services and agency outreach, related data collection efforts, to request support and technical assistance, to provide feedback, and/or to share lessons learned/challenges please contact DHS Federal Network Resilience:

CyberLiaison@hq.dhs.gov

Future Events

Webinar schedule:

Wednesday, September 5 - 1:00 pm – 2:30 pm (Eastern time)

Additional webinars may be scheduled if necessary.

Adobe Connect Webinar

https://dhsconnect.connectsolutions.com/FPKICertificateStore/

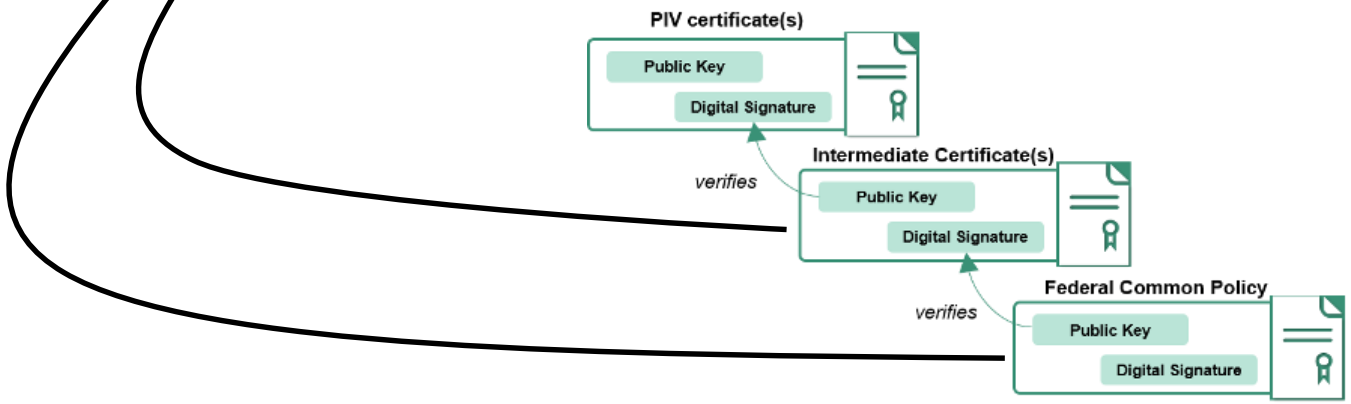
Dial In

1-855-852-7677 Access code: 9999 2977 3169#

Background

What is a Certification Authority?

- A Certification Authority (CA) is a trusted resource responsible for issuing and managing digital certificates.
- CAs are divided into two categories:
  - **Root CAs -** Sign Intermediate CAs
  - **Intermediate CAs -** Issue person/device certificates (called “end-entities”)



- The Federal Public Key Infrastructure (FPKI) is composed of over two hundred CAs, with the Federal Common Policy CA as the **root** distributed in the certificate stores.

What are certificate stores?

- Certificate stores tell operating systems and applications what certificates to trust.
- These stores contain lists of trusted **root** CA certificates.
- Using certificate stores, operating systems and applications don't need to "trust" millions of end-entity certificates.
- When presented with a certificate, an operating system or application will check its certificate store to see if *that* certificate has a valid path to a trusted **root** certificate.

How does Apple manage its global stores?

- Apple distributes hundreds of trusted root CA certificates globally for each of its operating systems (macOS, iOS, tvOS, and watchOS)
  - Certificates are included in the *System Roots Keychain*
  - Updated via operating system security update process

- Enterprises (agencies) can manage additional *enterprise trusted* certificate stores for enterprise users and computers
  - Enterprise trusted or distrusted CAs are stored and managed separately than those distributed by Apple
    - *Login Keychain* — Certificates associated with the specific user account logged into a device.
    - *System Keychain* — Certificates associated with all user accounts on a device.

U.S. Government Root Certificate Removal

What is happening?

- In the release of macOS Mojave and iOS 12 (**estimated timeline September to October 2018**), the Federal Government will remove the Federal Public Key Infrastructure (PKI) Root Certification Authority (CA) certificate from Apple's globally distributed certificate stores

- Older operating system versions will **not** be affected
- The root is known as the "Federal Common Policy CA"
  - Often referred to as "COMMON"
  - Also shown as "U.S. Government Root CA"
- The change will impact all federal agencies using Apple devices
- The impacts can be mitigated
- **Target date for mitigation actions: August 31, 2018**

Why is this happening?

- Commercial certificate stores (e.g., Microsoft and Apple) have strict requirements that trusted root CAs must follow to be *globally* distributed

- Federal PKI practices aren't consistent with required and emerging practices for *global* trust
  - Federal PKI is focused on the *federal enterprise* use cases

What will be affected?

- Affected implementations and services may include:
  - Personal Identity Verification (PIV) credential **authentication to the networks**
  - VPN authentication by users (SSL and IPsec)
  - Agency web application client authentication (users)
  - Validation of digital signatures in emails and documents, and
  - Other applications that rely on Apple's certificate stores

Plan of Action

How can I prevent issues?

- You'll need to install COMMON as a trusted root certificate on all government-furnished Apple devices.
- **<u>You can start this today.</u>**
  - Don't wait to see if the update breaks anything!
  - Open change requests and start processes.
- Procedures for government network domains:
  1. Download a copy of COMMON
  2. Verify your copy of COMMON
  3. Redistribute COMMON using an option below:
     a) Create, deploy, and install an Apple Configuration Profile (automated)
     b) Using Apple system tools (manual)
     c) Using third-party tools (automated or manual)

Who needs to hear about this?

- This requires collaboration and coordination across a variety of agency stakeholders:
  - Domain Administrators
  - Website / Application Administrators
  - Mobile Device Management Administrators

- Identify who you need to communicate with!

- Start communications **now**!

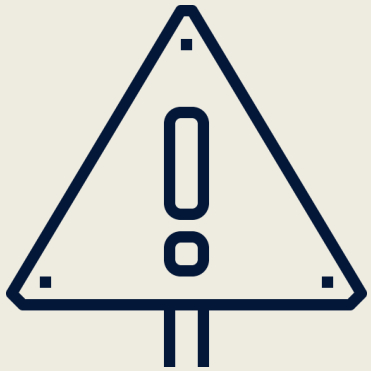
Solutions

Obtain a copy of COMMON

- Two options:
  1. Download from http://http.fpki.gov/fcpca/fcpca.crt
  2. Email fpki@gsa.gov to request an out-of-band copy
- Certificate details to support verification:

Federal Common Policy CA (FCPCA/COMMON)	Certificate Details
Distinguished Name	cn=Federal Common Policy CA, ou=FPKI, o=U.S. Government, c=US
Serial Number	0130
SHA-1 Thumbprint (digest/hash)	90 5f 94 2f d9 f2 8f 67 9b 37 81 80 fd 4f 84 63 47 f6 45 c1
SHA-256 Thumbprint (digest/hash)	89 4e bc 0b 23 da 2a 50 c0 18 6b 7f 8f 25 ef 1f 6b 29 35 af 32 a9 45 84 ef 80 aa f8 77 a3 a0 6e

Stop and Verify!



WARNING: You should **never** install a root certificate without verifying the digest.

Calculate hash and verify copy of COMMON

- Verify certificate details and digest/hash match the expected values shown on previous slide

- Using Terminal (macOS):
  1. Click the **Spotlight** icon and search for *terminal*.
  2. Double-click the **Terminal** icon (black monitor icon with white ">_") to open a window.
  3. Run the following command:

     $ shasum -a 256 {DOWNLOAD_LOCATION}/fcpca.crt

     Note: Replace {DOWNLOAD_LOCATION} with the directory path where COMMON was downloaded.

Redistribute via Configuration Profile

- You can create an Apple Configuration Profile to redistribute and automatically install COMMON on your agency's government-furnished Apple devices.
- Configuration Profiles can be used on both macOS and iOS.
- We have a sample Configuration Profile that can be used to redistribute COMMON posted on our Playbooks website.
- The steps on the following slide detail one method for creating a Configuration Profile using Apple's free *Configurator* 2 application.
  - Third-party applications can also be used to create, distribute, and automatically install profiles to managed Apple devices.

Create a Configuration Profile

Using *Configurator 2* on macOS:

The following steps will create a Configuration Profile, and are intended to be run by system or Mobile Device Management (MDM) administrators.

1. Download and install *Configurator 2* from the Apple App Store.
2. Open *Configurator 2* and click **File** -> **New Profile**.
3. Under the **General** tab…
   - Enter a unique profile **Name**. (e.g., “Federal Common Policy Certification Authority Profile”)
   - Enter a unique profile **Identifier**. (e.g., “FCPCA-0001”)
4. Under the **Certificates** tab…
   - Click **Configure,** then browse to and select your verified copy of COMMON.
5. [*Optional:* Add additional agency specific configurations.]
6. Click **File** -> **Save** to save your profile to a preferred file location.
7. Distribute the configuration profile to enterprise devices.

Distribute and Install Configuration Profile

Distribution Options:

- Over-the-air using a Mobile Device Management server.
- Over-the-air profile delivery and configuration.
- Share a profile on an agency intranet webpage**.***
- Email a profile to select agency users.*
- Use Apple's *Configurator 2* to distribute your Configuration Profile to government-furnished devices connected via USB.

[* Please see Slide 28 for an important note regarding iOS!**]**

Installation Options:

- Automatic (e.g., MDM automates installation without user intervention)
- Manual (e.g., user clicking on the distributed profile)

Distribution of Profiles for use with iOS

- iOS devices using a Configuration Profile distributed via an email or intranet site will require end-users to manually enable SSL trust (also referred to as “full trust”) for COMMON.

- These steps are outlined on the next slide (Slide 29).

- Where possible, automated distribution of Configuration Profiles via Mobile Device Management tools should be preferred to avoid manual procedures.

iOS - Manually Enable SSL Trust

Enable SSL trust:

The following steps will enable “full trust” for certificates chaining to COMMON, and are only necessary if a Configuration Profile is distributed via email or intranet site.

1. From the iOS device’s Home screen, go to **Settings** -> **General** -> **About** -> **Certificate Trust Settings**.
2. Beneath **Enable Full Trust for Root Certificates**, toggle trust **ON** for the Federal Common Policy CA certificate entry.
3. When the confirmation appears, click **Continue**.
4. You can now successfully navigate to any intranet website whose SSL certificate was issued by a Federal PKI CA.

Unmanaged Device Procedures

- We have manual procedures for redistributing COMMON to macOS and iOS devices on our Playbooks site.

- When possible, automated solutions should be exercised and are recommended by Apple.

Redistribute using Third-Party Tools

- Third-party configuration management applications already procured by your agency may include capabilities to redistribute COMMON as a trusted root CA.
  - Mobile Device Management tools support this
  - Apple recommends using Mobile Device Management tools to manage both iOS and macOS devices

- If you have any questions regarding a specific vendor or product, please contact fpki@gsa.gov and we will attempt to provide support.

FAQs

Frequently Asked Questions

Question: Where can I learn more?

Visit the Playbooks website.

- Teams are updating with questions and new information to support your needs.
- Stay tuned and check back often!

Frequently Asked Questions

Question: If I redistribute COMMON today, will it get erased when I update to the next major release of my Apple device's operating system?

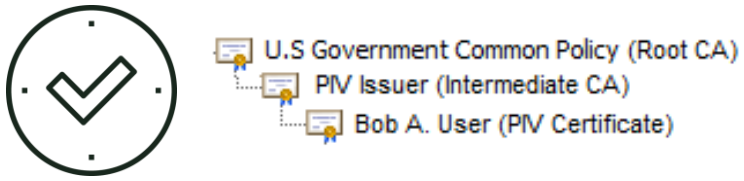
No, it will not be erased. We have verified this on both macOS and iOS. You can redistribute COMMON **today**.

Frequently Asked Questions

Question: Can you explain this change to me in a different way?

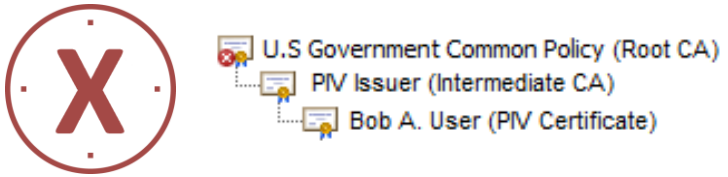
Current State

With our current distribution of COMMON in Apple's certificate stores, certificates issued from the Federal PKI can be validated to a known root certification authority.



Future State

Upon our removal of COMMON from Apple's certificate stores, certificates issued from the Federal PKI will no longer be validated to a known root certification authority.



Failure to successfully validate a certificate's chain will prevent authentication and digital signature validation.

We can prevent errors by redistributing COMMON.

Frequently Asked Questions

Question: What happens if I don't distribute COMMON?

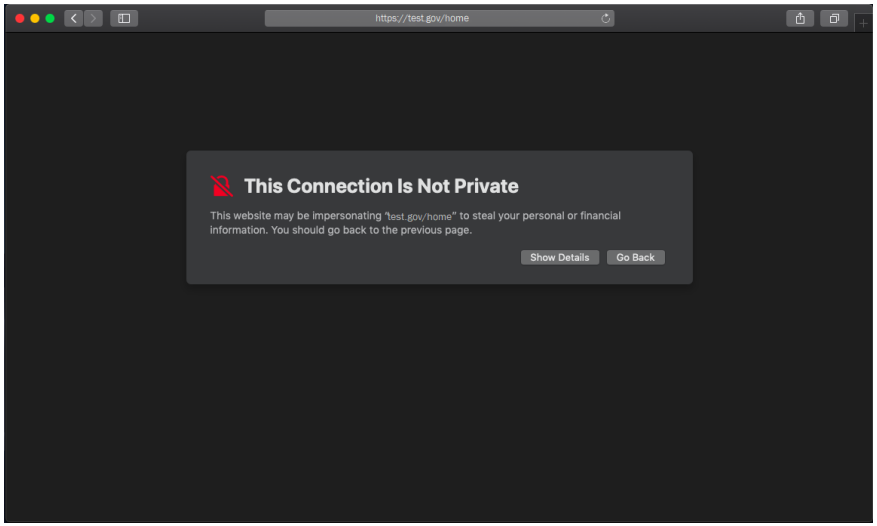
1. **Authentication issues (*High Impact*)**
   - Workstations
   - Websites
   - Applications (internal or cross-agency)
   - VPNs

2. **Error fatigue (*Medium Impact*)**
   - Removal of COMMON could result in unexpected application errors or system behavior for legacy and GOTS products

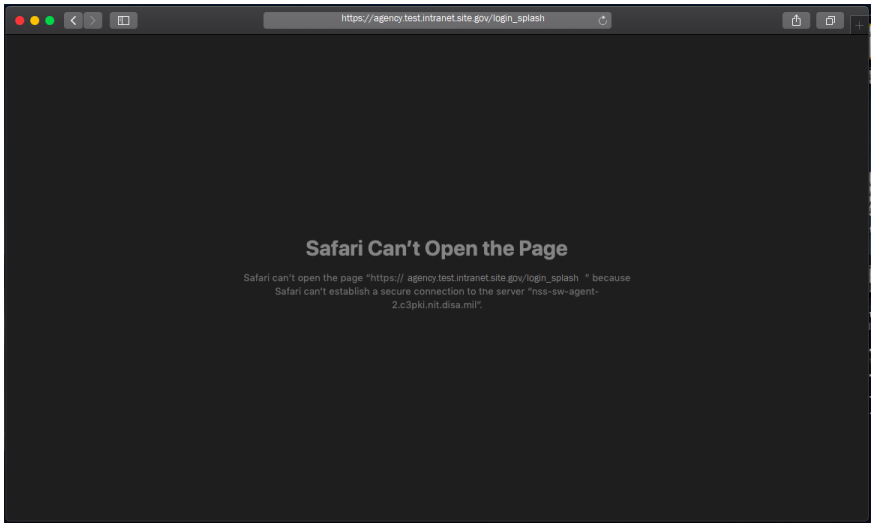
3. **Digital signature validation (*Low Impact*)**
   - Email
   - Documents and files (e.g., Microsoft Word)

Frequently Asked Questions

Question: Can you provide an example of what errors might look like if I do not redistribute COMMON (macOS)?



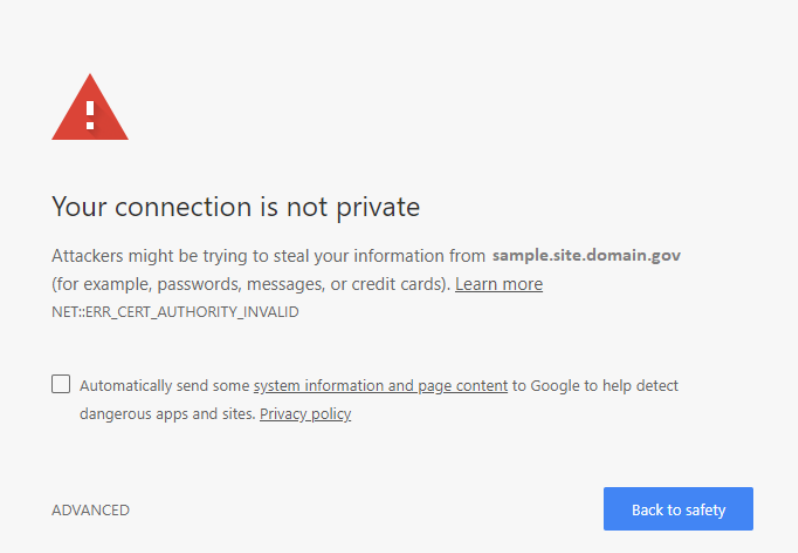
Sample error in Safari while navigating to an intranet site whose SSL/TLS certificate does not chain to a trusted root CA



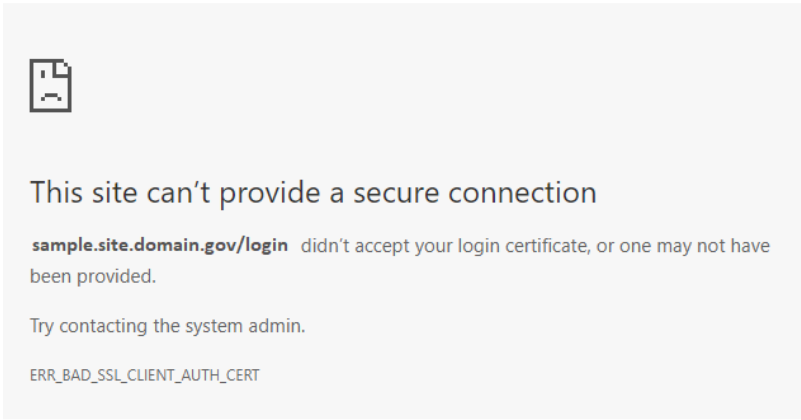
Sample error in Safari where client (PIV) authentication fails due to a user's certificate not chaining to a trusted root CA

Frequently Asked Questions

Question: Can you provide an example of what errors might look like if I do not redistribute COMMON (macOS)?



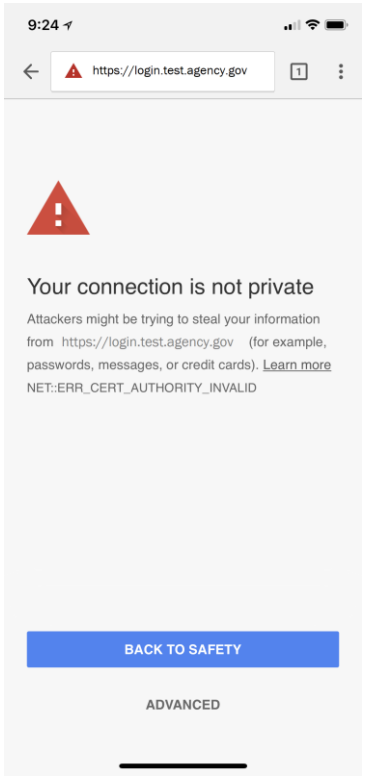
Sample error in Chrome while navigating to an intranet site whose SSL/TLS certificate does not chain to a trusted root CA



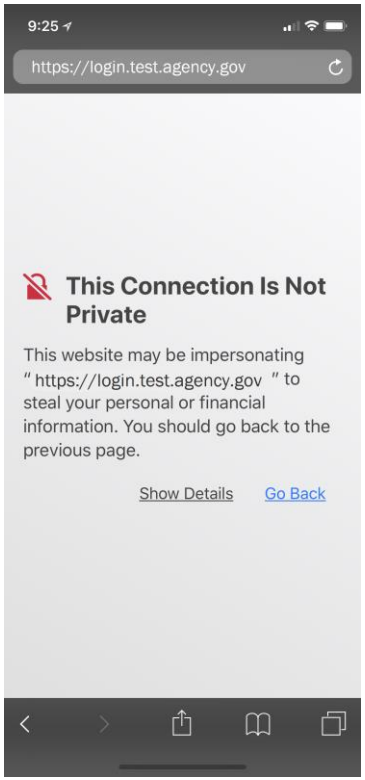
Sample error in Chrome where client (PIV) authentication fails due to a user's certificate not chaining to a trusted root CA

Frequently Asked Questions

Question: Can you provide an example of what errors might look like if I do not redistribute COMMON (iOS)?



Sample error in Chrome while navigating to an intranet site whose SSL/TLS certificate does not chain to a trusted root CA



Sample error in Safari while navigating to an intranet site whose SSL/TLS certificate does not chain to a trusted root CA

Frequently Asked Questions

Question: Which Apple products will be affected?

Affected Apple Operating System Versions		
macOS	**iOS**	**tvOS**
Mojave (10.14)	iOS 12	tvOS 12

Note: Older versions will not be affected by this update. If you have other Apple operating systems installed in your environment (e.g., watchOS), please let us know!

Frequently Asked Questions

Question: Is COMMON changing?

No.

COMMON's certificate will not change. The only change will be in how COMMON is distributed to devices.

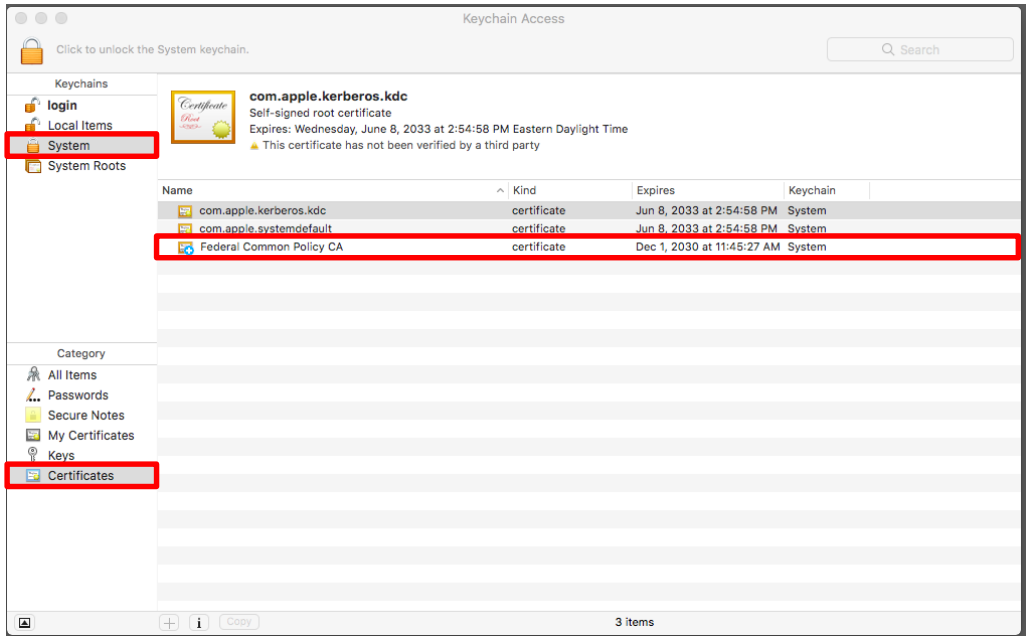
Frequently Asked Questions

Question: How can I verify that COMMON has been redistributed to my system (macOS)?

1. Click the **Spotlight** icon and search for *Keychain Access*.

2. Double-click the **Keychain Access** icon.

3. Ensure an entry for COMMON exists in either the **login** or **System** keychain *Certificates* repository.

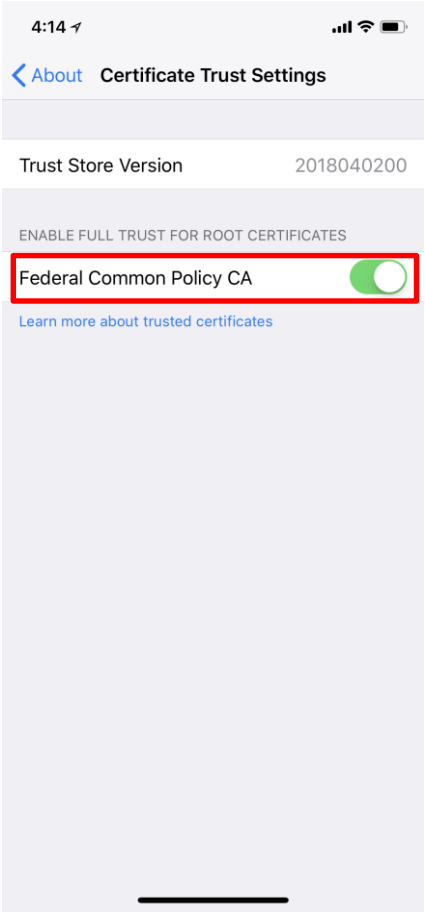


Frequently Asked Questions

Question: How can I verify that COMMON has been redistributed to my system (iOS)?

1. Navigate to…
   - **Settings**
   - **About**
   - **Certificate Trust Settings**

2. Then, verify that the Federal Common Policy CA is listed with “full trust”.



Frequently Asked Questions

Question: Can multiple copies of COMMON coexist in my certificate store?

Yes!

An enterprise distributed copy of COMMON will not conflict with the Apple distributed copy.

Frequently Asked Questions

Question: Should I be concerned with "Bring Your Own Device" (BYOD) program devices?

If BYOD program users are performing any of the following activities, redistributing COMMON is required to avoid issues:

- PIV smart card logon (to VPNs or intranet sites)
- Validate PIV digital signatures (emails or documents)
- Navigate to intranet pages whose SSL/TLS certificates chain to COMMON

Frequently Asked Questions

Question: My agency gets PIV cards from [Issuer Name]. I won't be affected by this, right?

Incorrect.

Your PIV credential issuer has no impact on whether your agency is affected by this change.

The impact is related to how COMMON is distributed to federal enterprise devices by agency-specific configuration management practices. It is not related to how *credentials* are generated or issued.

Frequently Asked Questions

Question: Will my PIV credentials break or need to be updated when this change happens?

No.

PIV credentials will not break, need to be updated, or replaced. Our credentials will not be changing or affected by this update.

Frequently Asked Questions

Question: How can I test the impact of the Federal Common Policy CA's (COMMON) removal?

If interested in learning more about Apple's public beta test program, please contact us at fpki@gsa.gov.

Open Discussion

Conclusion

Questions and Resources

Details and updated information on the removal of Federal PKI trust from the Apple certificate stores are maintained here: https://fpki.idmanagement.gov/truststores/apple/

For general inquiries on DHS services and agency outreach; related data collection efforts; to request support and technical assistance; to provide feedback; and/or to share lessons learned/challenges, please contact DHS Federal Network Resilience: CyberLiaison@hq.dhs.gov.

For technical inquiries and recommended actions, please contact GSA FPKI teams at fpki@gsa.gov.

To sign up for future communications regarding the removal of the COMMON from commercial certificate stores, send an email with your full name, email, agency, and sub-agency/component name to: fpkitruststoreremoval@gsa.gov.

Future Events

Webinar schedule:

Wednesday, September 5 - 1:00 pm – 2:30 pm (Eastern time)

Additional webinars may be scheduled if necessary.

Adobe Connect Webinar

https://dhsconnect.connectsolutions.com/FPKICertificateStore/

Dial In

1-855-852-7677 Access code: 9999 2977 3169#