Homeland Security

DHS Federal Network Resilience

Federal PKI Trust Removal from Microsoft Certificate Store

July 17, 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.

Welcome

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

- The change will impact all federal agencies across multiple services

- GSA, in coordination with DHS, supporting remediation efforts

- Target date for remediation December 31, 2018

Listserv

To receive updates on the removal of FPKI 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 Microsoft certificate store will be maintained here:

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

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:

Thursday, August 2, 2018 – 1:00 pm – 2:30 pm (Eastern time)

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/

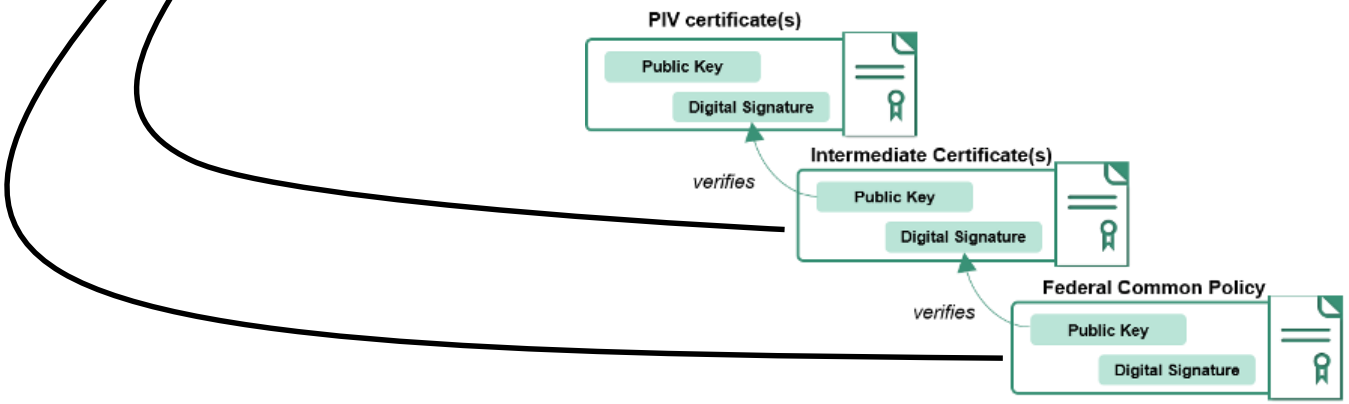
Dial In

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 Microsoft manage its global store?

- Microsoft distributes hundreds of trusted root CA certificates globally
  - Microsoft updates the root CA certificates using an auto-update process
  - Similar to *patch Tuesdays* - but a separate process!
  - This certificate store is called “AuthRoot”
  - This certificate store *should not* be modified by enterprise admins

- 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 Microsoft
  - These certificate stores are called “Enterprise Trust”

U.S. Government Root Certificate Removal

What is happening?

- In early 2019, the Federal Government will remove the Federal Public Key Infrastructure (PKI) Root Certification Authority (CA) certificate from Microsoft's globally distributed certificate store
- 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
- The impacts can be mitigated
- **Target date for mitigation actions: December 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)
  - Authentication to Office 365 (possibly)
  - Agency web application client authentication (users)
  - Digital signatures in Word documents, and
  - Other applications that rely on Microsoft's certificate store

Plan of Action

How can I prevent issues?

- You'll need to install COMMON as a trusted root certificate on all government-furnished, Windows workstations and devices.
- **You can start this today.**
  - 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 any of these options:
     a. Microsoft certutil
     b. Microsoft Group Policy Object (GPO)
     c. Third-party configuration management tools
     d. Manually using Microsoft Certificate Manager
- Review your services built on Microsoft servers (physical, virtual, or cloud).

Solutions

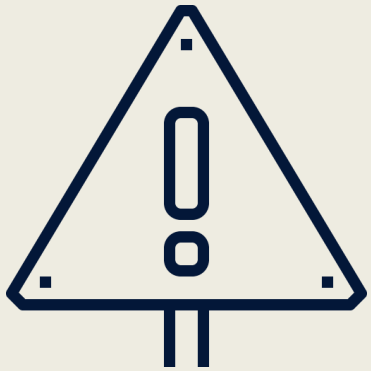
Obtain a copy of COMMON

- 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

- Using one of the methods below, verify certificate details and digest/hash match the expected values shown on previous slide
- Microsoft command line via certutil:
  1. Click **Start**, type **cmd**, and press **Enter**
  2. Run command:
     > certutil -hashfile [PATH\]fcpca.crt SHA256
- Microsoft command line via OpenSSL:
  1. Click **Start**, type **cmd**, and press **Enter**
  2. Run command:
     > openssl sha256 [PATH\]fcpca.crt
- Microsoft PowerShell:
  1. Click **Start**, type **PowerShell**, and press **Enter**
  2. Run command:
     > Get-FileHash [PATH\]fcpca.crt | Format-List

Redistribute COMMON via certutil (Option 1)

- To redistribute COMMON, you must have Enterprise Administrator privileges
- These procedures are for Active Directory environments
- From an agency Domain Controller:
  1. Click **Start**, type **cmd**, and press **Enter**
  2. Run command:

     > certutil -dspublish -f [PATH\]fcpca.crt RootCA
- Verify that COMMON was distributed:
  1. Run commands:

     > gpupdate /force

     > certutil -viewstore -enterprise
  2. Confirm that COMMON is contained in the output details
  3. [OPTIONAL] Verify the certificate details against expected values (e.g., serial #)

Redistribute COMMON via GPO (Option 2)

- To redistribute COMMON via GPO, you must have Enterprise Administrator privileges
- From an agency Domain Controller:
  1. Navigate to **Server Manager**
  2. Select **Tools**
  3. Select **Group Policy Management** from the drop-down list
  4. Right-click your desired domain(s) and select **Create a GPO in this domain**, and **Link it here…**
  5. Enter a GPO **Name** and click **OK**
  6. Right-click the newly created GPO and click **Edit…**
  7. Navigate to **Policies** -> **Windows Settings** -> **Security Settings** -> **Public Key Policies** …. ***(continued…)***

Redistribute COMMON via GPO (Option 2)

8. Right-click **Trusted Root Certification Authorities**, and select **Import**
   The Certificate Import Wizard will open

9. Browse to and select your copy of COMMON

10. Verify that the target **Certificate Store** presents **Trusted Root Certification Authorities**, and select **Next**

11. Select **Finish** to complete the import

    Confirmation message: The import was successful

12. Close the **Group Policy Management** window

13. [OPTIONAL] Wait for clients to consume the new policy or force consumption:

    1. Click **Start**, type **cmd**, and then press **Enter**
    2. Run command:
       > gpupdate /force

Redistribute via third-party tools (Option 3)

- You can use third-party configuration management tools, such as BigFix

  1. Using BigFix, schedule a task and push the certificate file.
  2. Run command (example):

     > certutil -f -addstore root "fcpca.crt"

Redistribute manually (Option 4)

- For unmanaged devices, manual procedures may be required
  1. Click **Start**, type **certmgr.msc**, and then press **Enter**
  2. Right click **Trusted Root Certification Authorities** and select **All Tasks** -> **Import**
     The Certificate Import Wizard will open
  3. Browse to and select your copy of COMMON
  4. Verify that the target **Certificate Store** presents **Trusted Root Certification Authorities**, and select **Next**
  5. Select **Finish** to complete the import

     Confirmation message: The import was successful

Note: If multiple users share a device, running **certlm.msc** instead of **certmgr.msc** will allow administrators to update all user account certificate stores at once, rather than requiring a separate import for each individual user account.

FAQs

Frequently Asked Questions

Question: Where can I learn more?

Visit the Playbooks site.

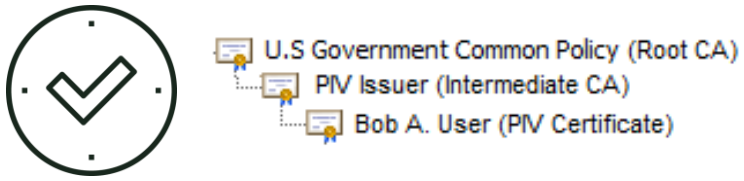
- Teams are updating with questions and new information to support your needs.
- We have posted screen captures of the technical solutions described in this webinar.
- Stay tuned and check back often!

Frequently Asked Questions

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

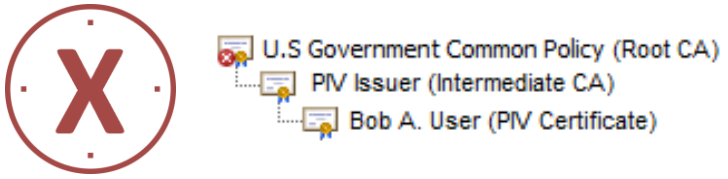
Current State

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



Future State

Upon our removal of COMMON from Microsoft's certificate store, 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?

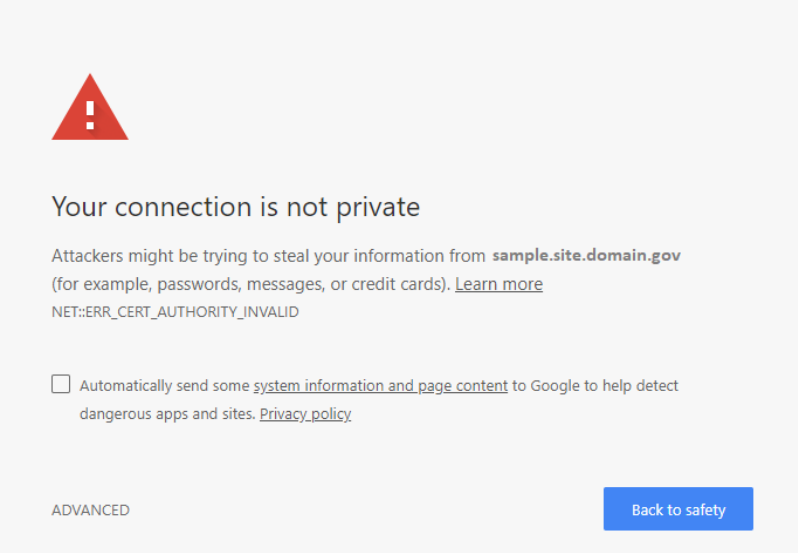
1. **Authentication issues (*High Impact*)**
   - Workstations
   - Websites
   - Applications (internal or cross-agency)
   - VPNs

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

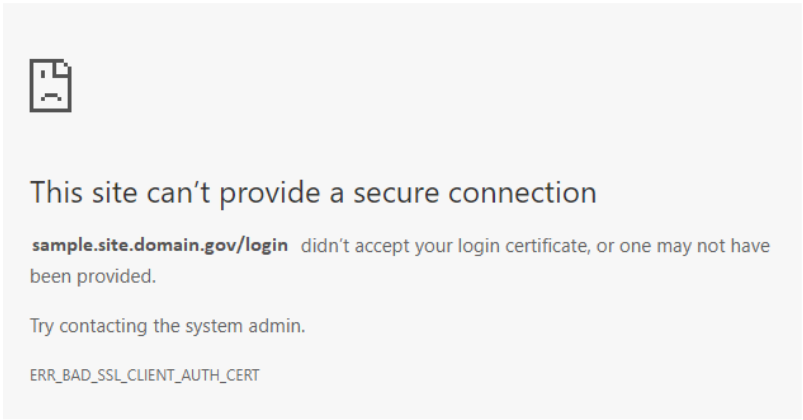
3. **Digital signature validation (*Low Impact*)**
   - Email
   - Documents and files (e.g., Microsoft Word)

Frequently Asked Questions

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



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

Sample error in Outlook where a signed email does not chain to a trusted root CA

Frequently Asked Questions

Question: Which Microsoft products will be affected?

Affected Microsoft Operating System Versions	
Personal Computer	**Server**
Windows 10	Windows Server 2016
Windows 8.1	Windows Server 2012 R2
Windows 8	Windows Server 2008 R2
Windows 7	
Windows Vista	

Note: if you have other versions of Windows installed in your environment, 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.

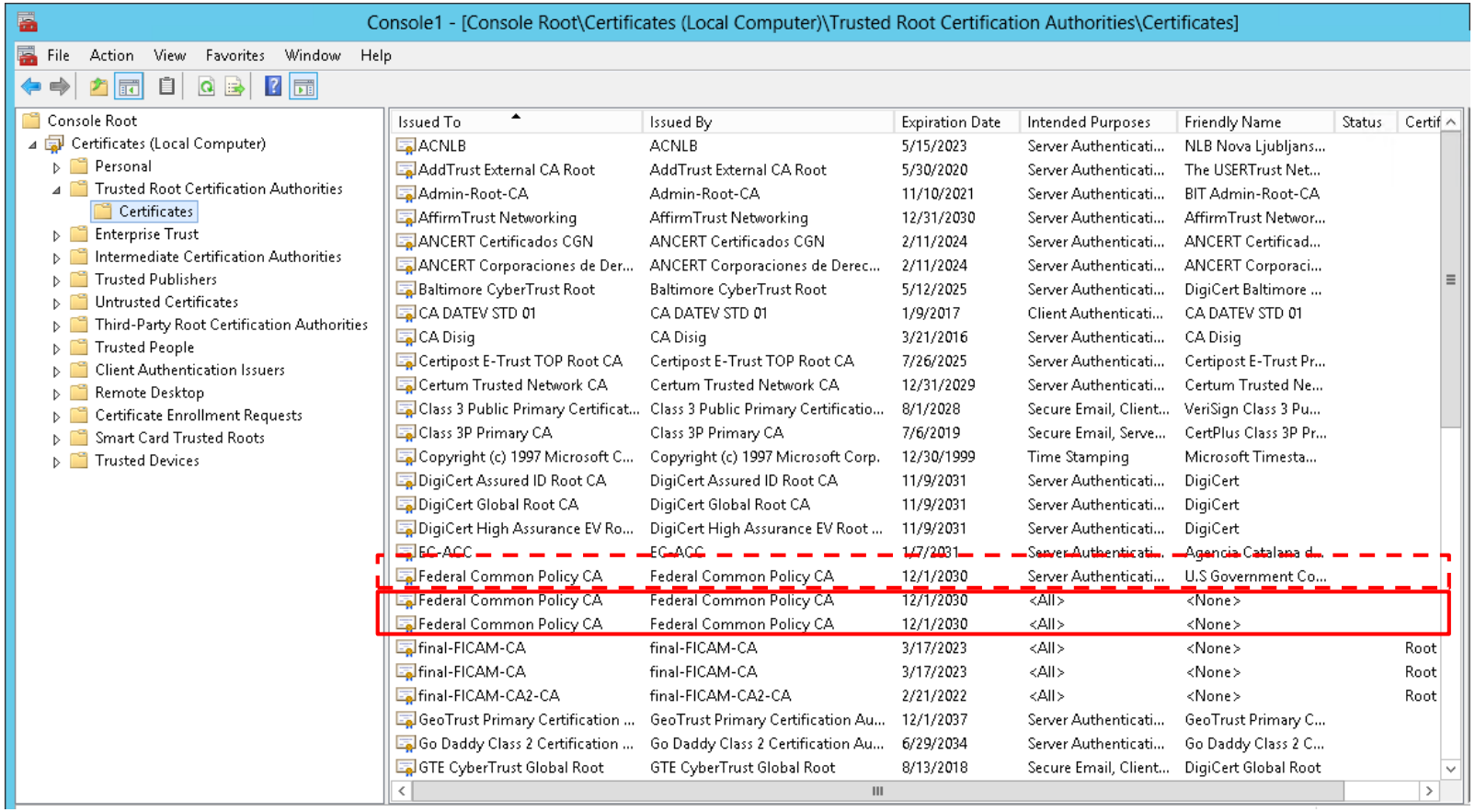
Frequently Asked Questions

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

1. Open Microsoft Certificate Viewer
   - **Start**, type **certmgr.msc**, and then press **Enter**

2. Navigate to **Trusted Root Certification Authorities** -> **Certificates**
   - You may see two (or more) copies of COMMON, depending on how it is being distributed.
     - Typically, enterprise distributed copies will be presented with an **Intended Purposes** value of **<ALL>** and a **Friendly Name** of **<None>**
     - CTL distributed copies will be presented with multiple **Intended Purposes** values and a **Friendly Name** of **U.S. Government Common Policy**
   - This is depicted on the following slide

Frequently Asked Questions



In the screenshot above, we see three entries for COMMON.

- The first entry (surrounded by a “dashed” line) is being populated from the Microsoft CTL. Note the values associated with **Intended Purposes** and **Friendly Name**.
- The remaining two entries resulted from following procedures in this presentation.

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 Microsoft 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 Microsoft's removal of the Federal Common Policy CA (COMMON)?

It is possible to simulate the Microsoft certificate store's future state. It is not recommended due to the potential for destructive outcomes.

If interested in learning more, 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 Microsoft certificate store are maintained here: https://fpki.idmanagement.gov/truststores/microsoft/

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:

Thursday, August 2, 2018 – 1:00 pm – 2:30 pm (Eastern time)

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#

Homeland Security