FERMILAB-SLIDES-19-031-CD

Fermilab U.S. DEPARTMENT OF ENERGY Office of Science

Implementing the Yubikey at Fermilab

Saúl González and Al Lilianstrom

National Laboratories Information Technology Summit 2019

This manuscript has been authored by Fermi Research Alliance, LLC under Contract No. DE-AC02-07CH11359 with the U.S. Department of Energy, Office of Science, Office of High Energy Physics.

Implementing the Yubikey at Fermilab

Fermilab, America's particle physics and accelerator laboratory, is an open science facility. Fermilab started limited use of DOE issued PIV-I cards for elevated access to services as part of the 2016 DOE mandate. With FIPS 140-2 validated Yubikeys now available Fermilab has begun a much broader implementation using the Yubikey as a PIV-I Smart Card, not only to replace the DOE issued cards, but to expand the usage to more users and services as well as network access.

This talk will cover Yubikey provisioning and lifecycle management, authentication service configuration, integration with existing applications and account lifecycle processes, and usage across the unique Fermilab infrastructure.

Track - Infrastructure/Operations

FERMILAB-SLIDES-19-031-CD

About Fermilab

Fermilab is America's particle physics and accelerator laboratory.

- Our vision is to solve the mysteries of matter, energy, space and time for the benefit of all. We strive to:
  - lead the world in neutrino science with particle accelerators
  - lead the nation in the development of particle colliders and their use for scientific discovery
  - advance particle physics through measurements of the cosmos

Our mission is to drive discovery by:

- building and operating world-leading accelerator and detector facilities
- performing pioneering research with national and global partners
- developing new technologies for science that support U.S. industrial competitiveness

www.fnal.gov

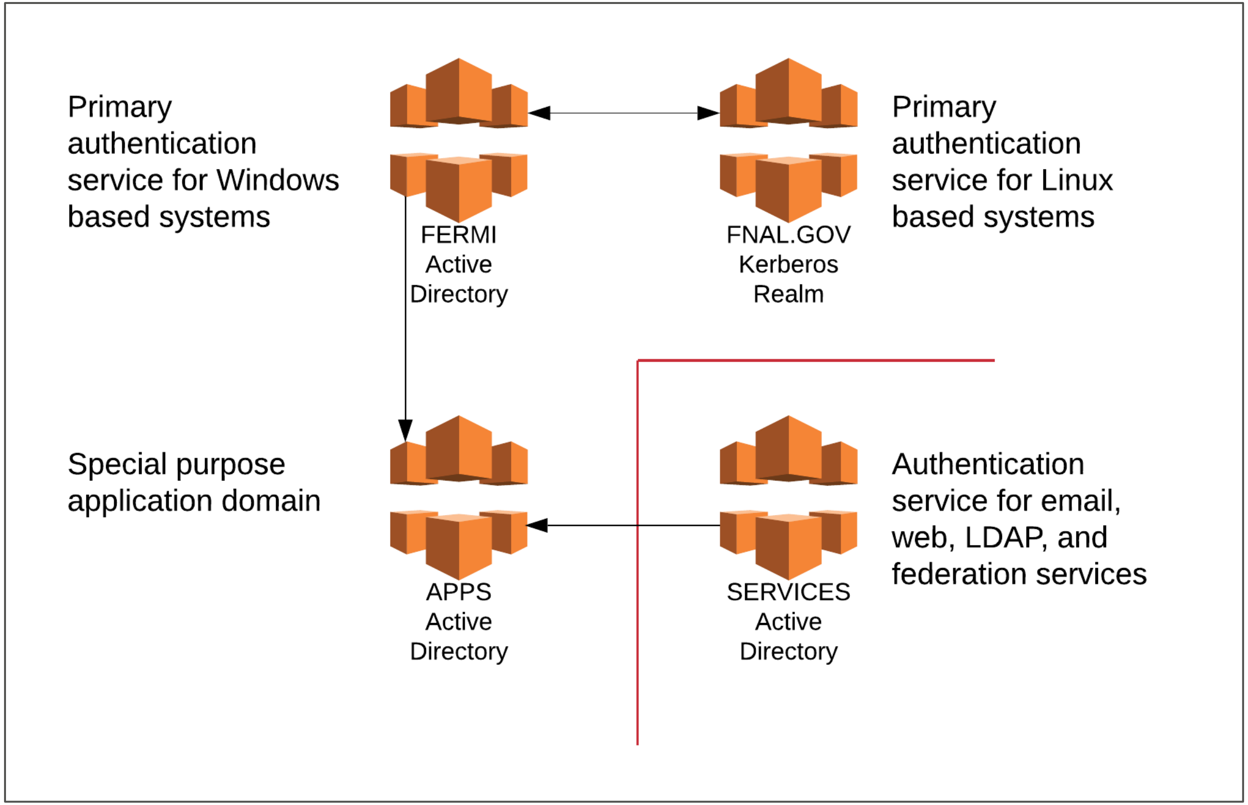
The Fermilab Environment

- Fermilab is an Open Science Laboratory
- Fermilab's 1,750 employees include scientists and engineers from all around the world.
  - Currently hosting over 4000 users
- Fermilab collaborates with more than 50 countries on physics experiments based in the United States and elsewhere.

Timeline

- PIV Rollout – September 2016
  - Focus on "privileged access"
    - Authentication admins
    - Network admins
    - PII
  - Small distribution
- HID ActiveKey evaluation – Summer 2017
  - Undertaken by the Authentication Services Group
    - Goal was to find an ActiveClient compatible smartcard for use with our Certificate Authority
- Yubikey evaluation – Fall 2017
- Yubikey rollout – Spring 2019

Authentication Overview



Primary authentication service for Windows based systems

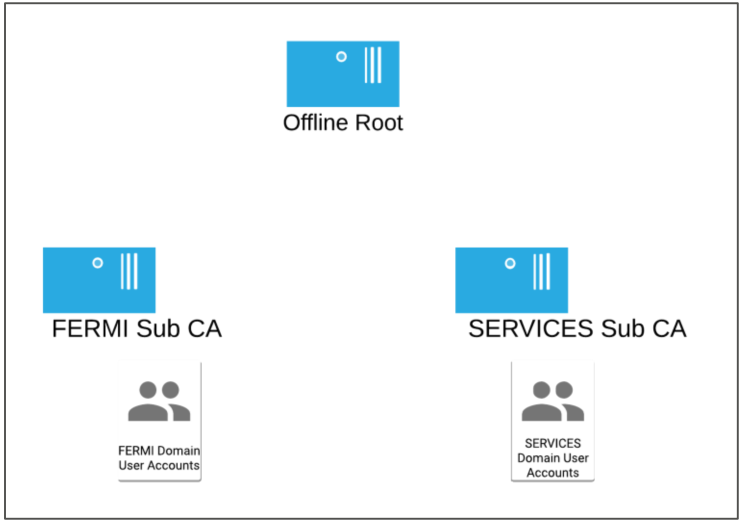
Primary authentication service for Linux based systems

Special purpose application domain

Authentication service for email, web, LDAP, and federation services

Infrastructure

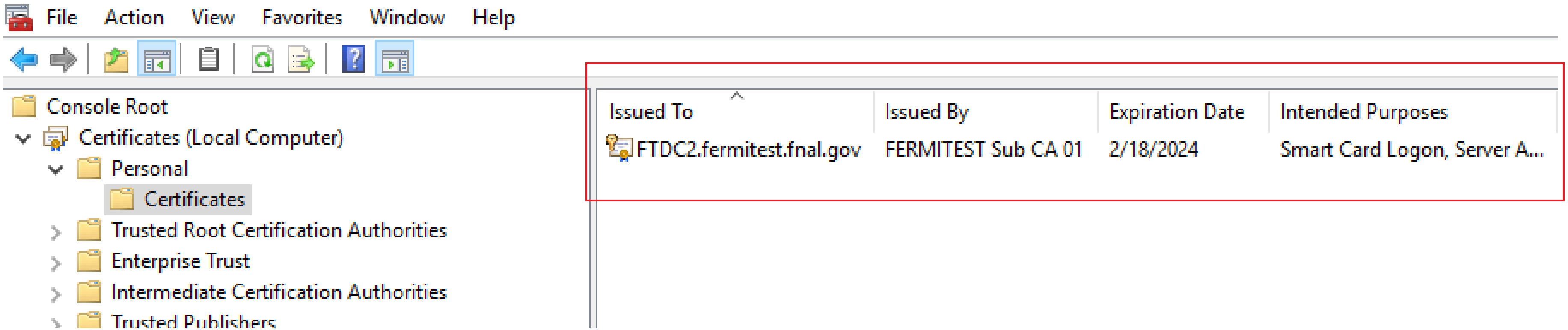
- Certificate Authority Servers
  - Microsoft Certificate Services integrated with Active Directory
    - Offline Root CA
    - Subordinate CAs for each Active Directory domain
      - User and computer certificates are issued from the subordinate CA
  - Certificates for the Root and Subordinate should be published to Active Directory to deploy to all domain members
  - Non-domain computers will have to add them
    - BYOD
    - Non-Windows
      - Managed and Stand-alone



Infrastructure

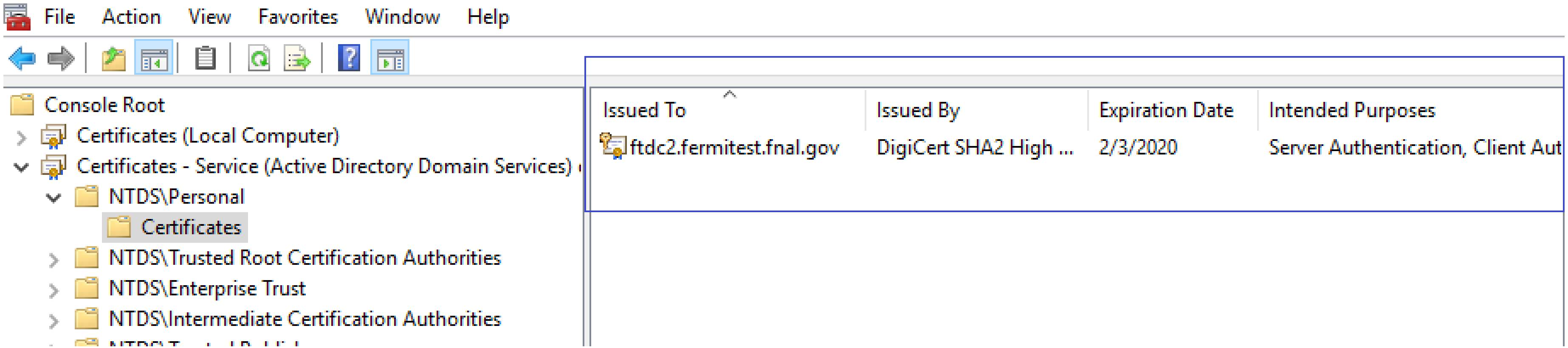
- Certificate Revocation List
  - CRLs are hosted on a central web server
    - CRLs are updated hourly on the subordinate CAs and copied to the web server with a PowerShell script
    - Offline Root CA CRL is published and copied to the central web server as part of the monthly patching process
    - Exception was required to site policy as a CRL must be located on a plain HTTP site
  - Certificates had to be reissued as the CRL evolved
    - Individual CA server
      - Central web server

Infrastructure



- Console Root
  - Certificates (Local Computer)
    - Personal
      - Certificates
    - Trusted Root Certification Authorities
    - Enterprise Trust
    - Intermediate Certification Authorities
    - Trusted Publishers

Issued To	Issued By	Expiration Date	Intended Purposes
FTDC2.fermitest.fnal.gov	FERMITEST Sub CA 01	2/18/2024	Smart Card Logon, Server A...



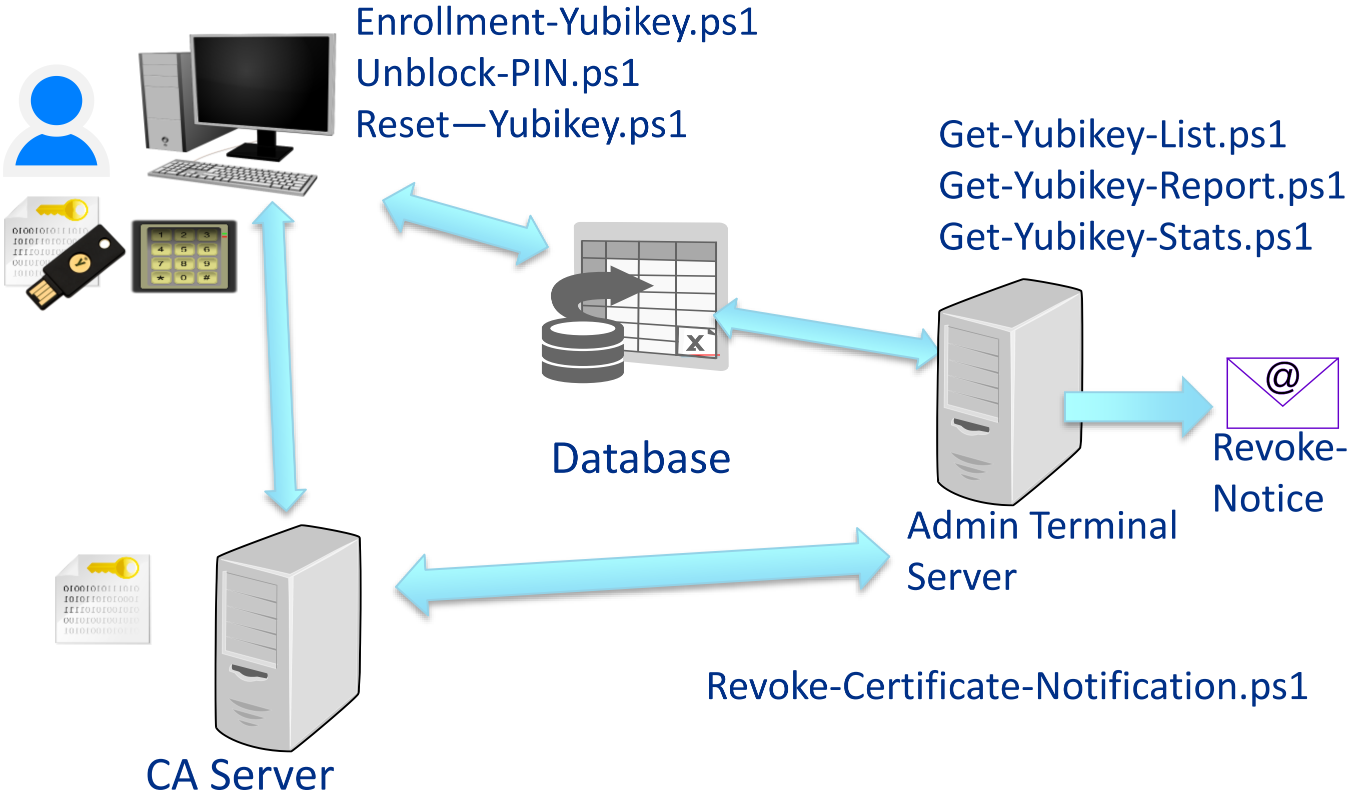
- Console Root
  - Certificates (Local Computer)
  - Certificates - Service (Active Directory Domain Services)
    - NTDS\Personal
      - Certificates
    - NTDS\Trusted Root Certification Authorities
    - NTDS\Enterprise Trust
    - NTDS\Intermediate Certification Authorities

Issued To	Issued By	Expiration Date	Intended Purposes
ftdc2.fermitest.fnal.gov	DigiCert SHA2 High ...	2/3/2020	Server Authentication, Client Aut

Yubikey

- Database
  - Yubikey serial number
  - PUK
  - Management key
  - Username
  - Management data
- Identity proofing
  - HR business process
  - Employees and on-premise contractors only at this time

Work Flow



Enrollment-Yubikey.ps1
Unblock-PIN.ps1
Reset—Yubikey.ps1

Get-Yubikey-List.ps1
Get-Yubikey-Report.ps1
Get-Yubikey-Stats.ps1

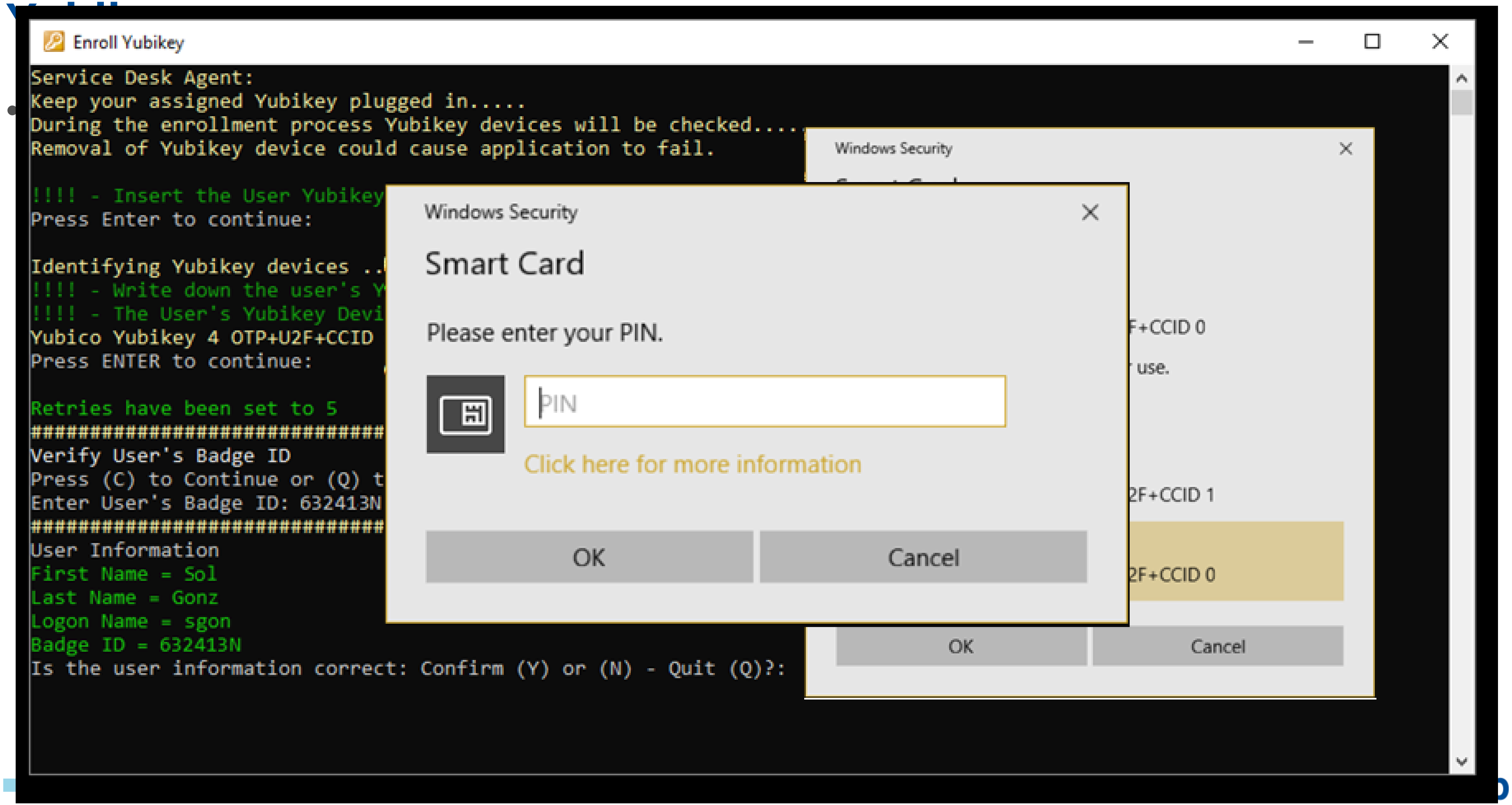
Database

Admin Terminal Server

Revoke-Notice

CA Server

Revoke-Certificate-Notification.ps1



Enroll Yubikey

```
Service Desk Agent:
Keep your assigned Yubikey plugged in.....
During the enrollment process Yubikey devices will be checked....
Removal of Yubikey device could cause application to fail.

!!!! - Insert the User Yubikey
Press Enter to continue:

Identifying Yubikey devices ..
!!!! - Write down the user's Y
!!!! - The User's Yubikey Devi
Yubico Yubikey 4 OTP+U2F+CCID
Press ENTER to continue:

Retries have been set to 5
##############################
Verify User's Badge ID
Press (C) to Continue or (Q) t
Enter User's Badge ID: 632413N
##############################
User Information
First Name = Sol
Last Name = Gonz
Logon Name = sgon
Badge ID = 632413N
Is the user information correct: Confirm (Y) or (N) - Quit (Q)?:
```

Windows Security

Smart Card

Please enter your PIN.

PIN

Click here for more information

Windows Security

F+CCID 0

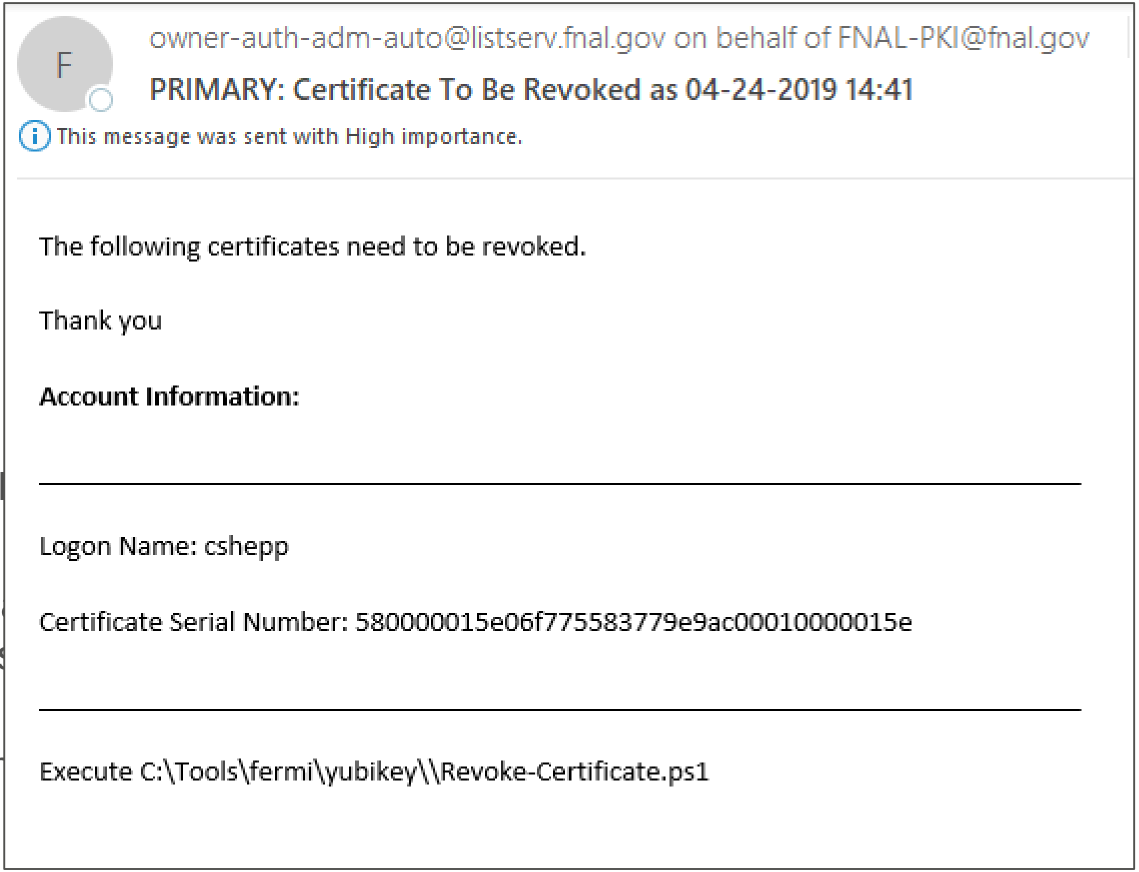
use.

2F+CCID 1

2F+CCID 0

Yubikey

- Other functions
  - Replacement
    - Lost or damaged
  - Clearing
    - Termination
  - Pin/PUK reset
    - Yubikey locks after 5 bad PI
  - With the Replacement or Cle previously issued certificate i Revocation Pending
    - PowerShell script queries th
      - Contacts CA and revokes
        - Updates database



owner-auth-adm-auto@listserv.fnal.gov on behalf of FNAL-PKI@fnal.gov

PRIMARY: Certificate To Be Revoked as 04-24-2019 14:41

This message was sent with High importance.

The following certificates need to be revoked.

Thank you

Account Information:

Logon Name: cshepp

Certificate Serial Number: 580000015e06f775583779e9ac00010000015e

---

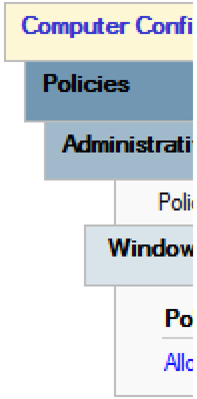
Execute C:\Tools\fermi\yubikey\\Revoke-Certificate.ps1

Uses

- Application servers
  - Windows
  - Linux
- Appliances

Application Servers

- Windows
  - Install Yubikey minidriver
    - Diffe



Computer Confi

Policies

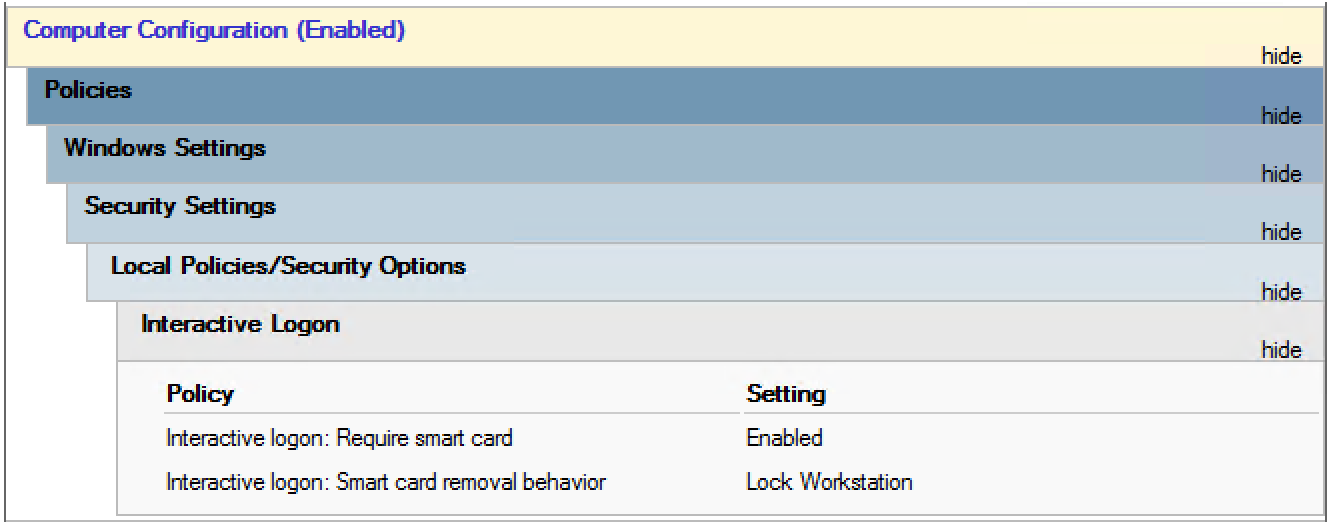
Administrati

Poli

Window

Po

Allo



Computer Configuration (Enabled) hide

Policies hide

Windows Settings hide

Security Settings hide

Local Policies/Security Options hide

Interactive Logon hide

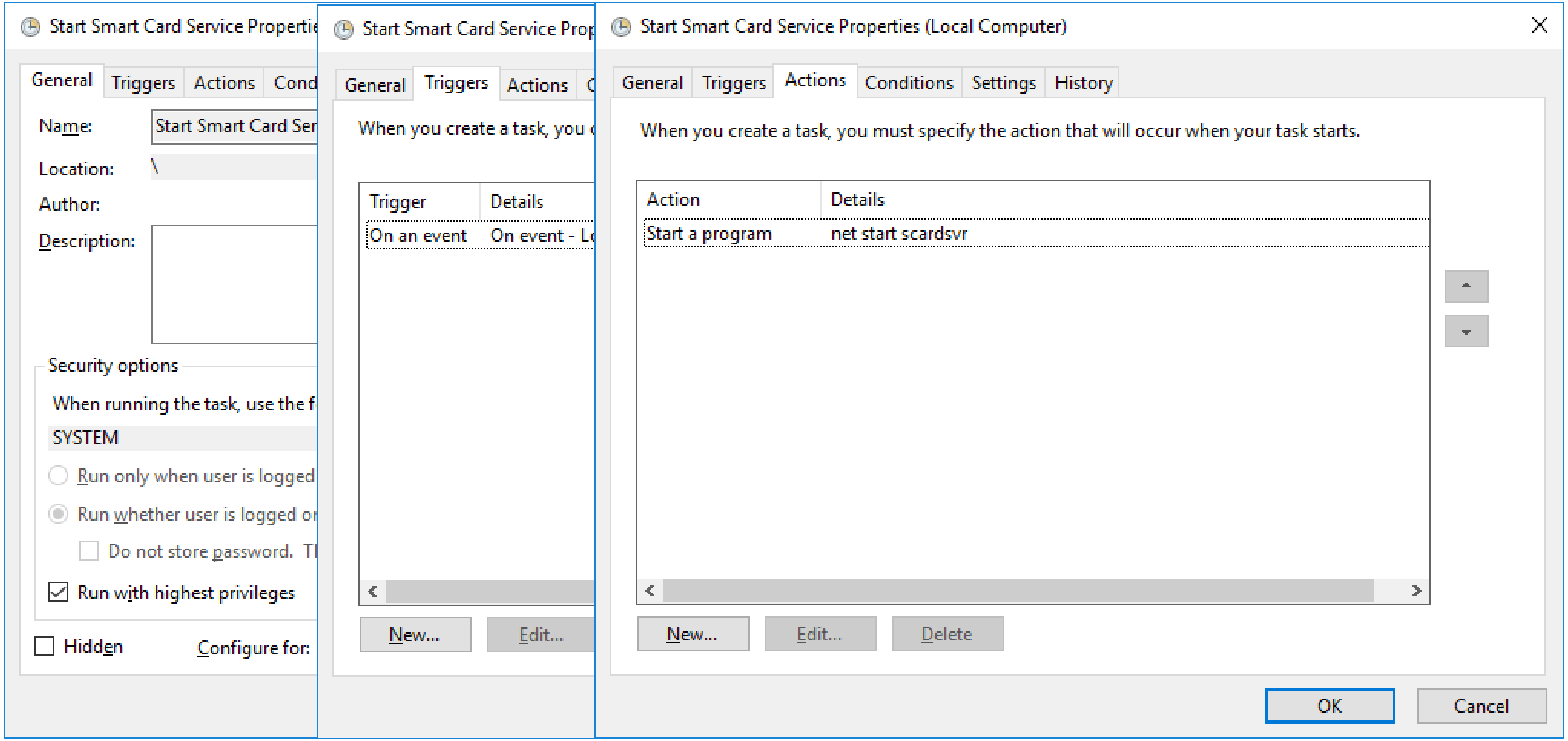
Policy	Setting
Interactive logon: Require smart card	Enabled
Interactive logon: Smart card removal behavior	Lock Workstation

Application Servers

- Clients for Windows Servers
  - Windows Remote Desktop
  - Microsoft Remote Desktop for OSX
  - rdesktop (OSX and Linux)
    - OSX – homebrew (https://brew.sh/)
      - brew install homebrew/x11/rdesktop --with-smartcard

Application Servers

-



Name: Start Smart Card Ser

Location: \

Author:

Description:

Security options

When running the task, use the f

SYSTEM

○ Run only when user is logged

● Run whether user is logged o

☐ Do not store password. Th

☑ Run with highest privileges

☐ Hidden

Configure for:

When you create a task, you c

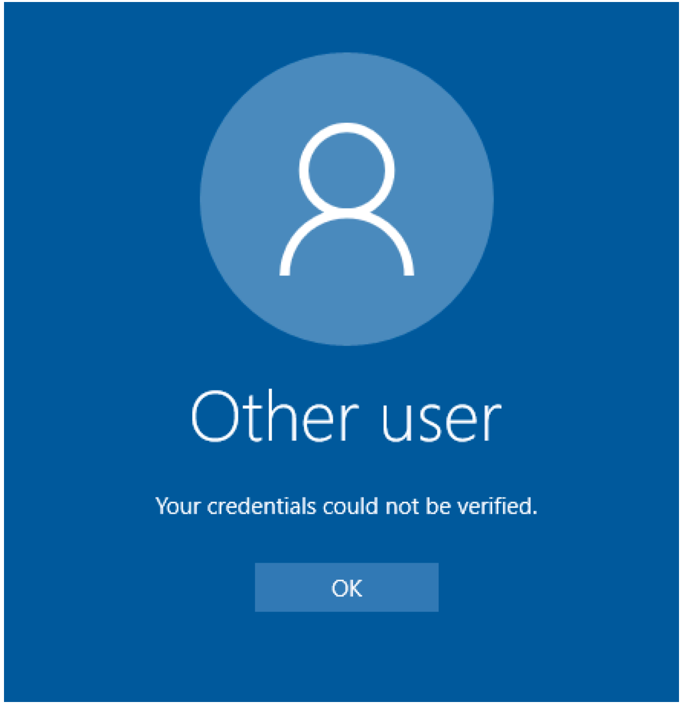
Trigger	Details
On an event	On event - Lo

When you create a task, you must specify the action that will occur when your task starts.

Action	Details
Start a program	net start scardsvr

Application Servers

- Windows
  - Certificate subject must be added to the altSecurityIdentities attribute for the user in Active Directory
    - Default access limited to Domain Admins
      1. Delegate access to the Service Desk personnel that issue the Yubikeys and have the issuing script update the attribute
      2. Delegate access to a service account that monitors the database and updates the attribute
      3. Monitor the database with a script and generate commands to be executed by the domain admins
    - Currently – option #3 is in use

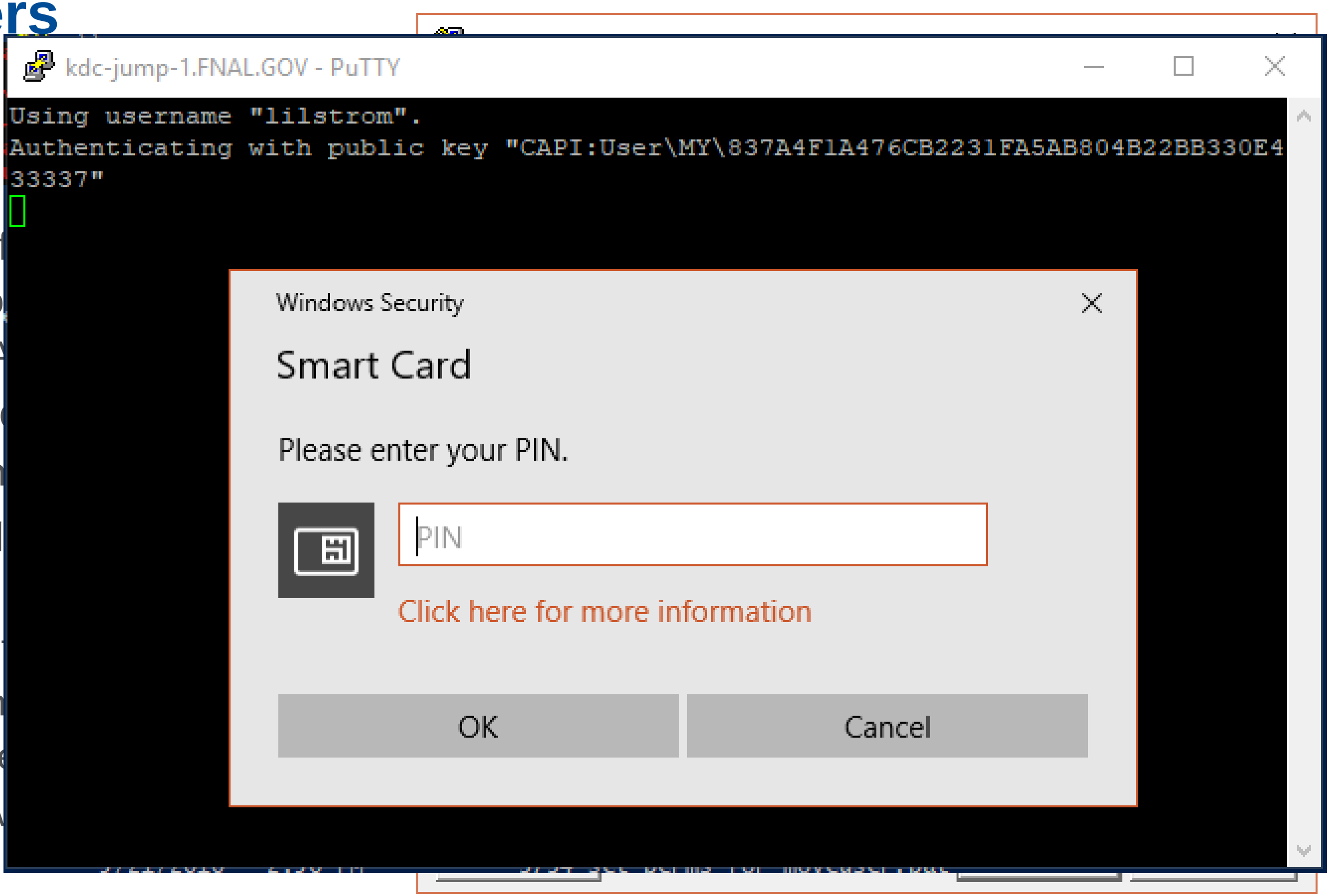


Other user

Your credentials could not be verified.

Application Servers

- Linux
  - Configure sshd
    - /etc/ssh/sshd_conf
      - Disable Kerbero
      - Enable PubkeyA
  - Coordinate with Cyb
    - Compliance scann
    - Exception was req
  - User configuration
    - Extract public key
      - Add to .ssh/auth
      - Be sure to set pe
    - PuTTY Users – a v
      - PuTTY-CAC



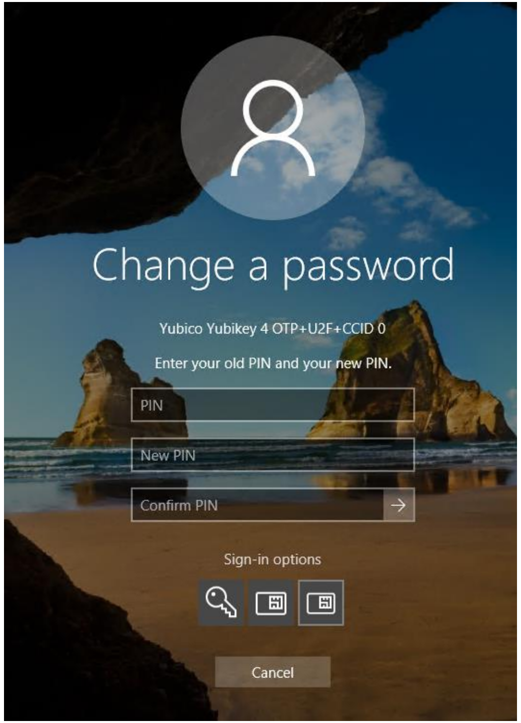
```
Using username "lilstrom".
Authenticating with public key "CAPI:User\MY\837A4F1A476CB2231FA5AB804B22BB330E4
33337"
```

Appliances

- VPN
  - MultiFactor authentication
- Citrix
  - Replace and extend the existing PIV usage

Remote locations

- Deep Underground Neutrino Experiment (DUNE)
  - Lead, South Dakota
- Provisioning
  - Videoconference assistance for issuing Yubikeys
    - Certificate on Yubikey will be on Hold in the CA so it can not be used
  - Remote user must contact the Service Desk once the Yubikey arrives to get the default PIN
    - Videoconference
  - Windows users will be able to reset PIN with Ctrl-Alt-Delete
    - OSX and Linux…



Change a password

Yubico Yubikey 4 OTP+U2F+CCID 0

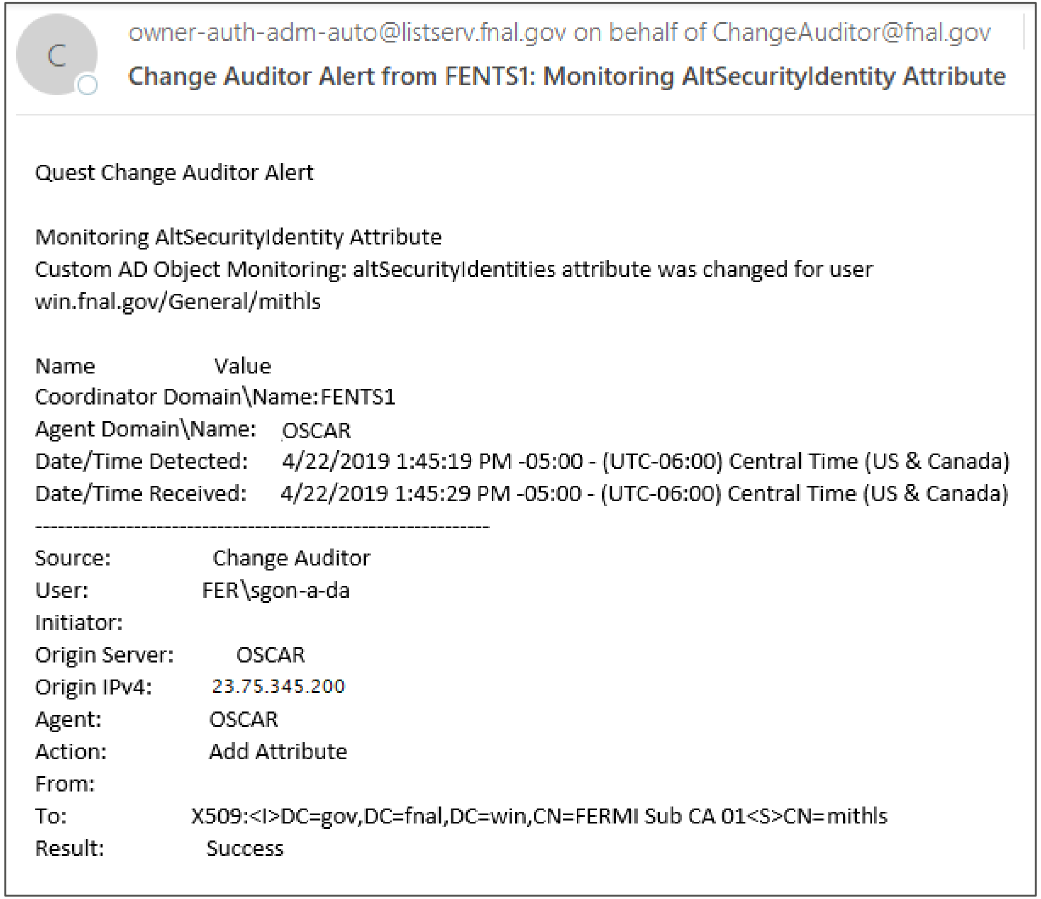
Enter your old PIN and your new PIN.

Remote locations

- User assistance
  - PIN Reset
  - Locked Yubikey

Monitoring

- altSecurityIdentities attribute
  - Certificates can be added to any account allowing access
    - Quest Change Auditor
      - Alerts domain administrators whenever the attribute is modified
    - PowerShell script
      - Checks the certificate assigned against the username of the account
        - Notifies domain administrators of any discrepancies



owner-auth-adm-auto@listserv.fnal.gov on behalf of ChangeAuditor@fnal.gov

Change Auditor Alert from FENTS1: Monitoring AltSecurityIdentity Attribute

Quest Change Auditor Alert

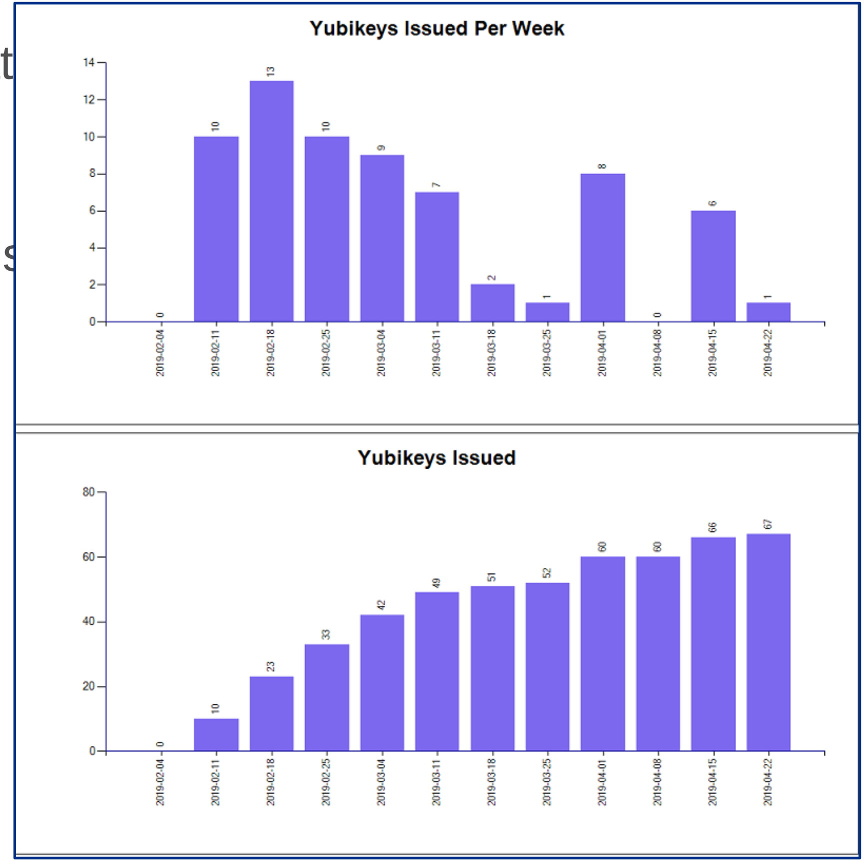
Monitoring AltSecurityIdentity Attribute
Custom AD Object Monitoring: altSecurityIdentities attribute was changed for user win.fnal.gov/General/mithls

Name	Value
Coordinator Domain\Name:	FENTS1
Agent Domain\Name:	OSCAR
Date/Time Detected:	4/22/2019 1:45:19 PM -05:00 - (UTC-06:00) Central Time (US & Canada)
Date/Time Received:	4/22/2019 1:45:29 PM -05:00 - (UTC-06:00) Central Time (US & Canada)

Source:	Change Auditor
User:	FER\sgon-a-da
Initiator:	
Origin Server:	OSCAR
Origin IPv4:	23.75.345.200
Agent:	OSCAR
Action:	Add Attribute
From:	
To:	X509:<I>DC=gov,DC=fnal,DC=win,CN=FERMI Sub CA 01<S>CN=mithls
Result:	Success

Metrics

- PowerShell script to query the dat
  - In the past week
  - Since issuance started
- PowerShell script to create graphs
  - Get-Corpchart PowerShell script
    - https://me.ahasayen.com/



Future plans

- Desktop logon
  - Get rid of passwords
- SSO Integration
  - Step up for certain URLs
  - MFA for select sites
- FNAL.GOV Kerberos realm integration

Lessons learned

- Use of the PIV is still required for access of the One ID web service
- Scheduled tasks running under service accounts on SmartCard required servers
  - If you need to start a command prompt as the service account your certificate needs to be added to the service accounts altSecurityIdentities attribute
    - This allows **runas /smartcard /user:domain\serviceaccount cmd** to work
      - Potential security issue
        - Monitor changes to altSecurityIdentities
- A revoked certificate on a Yubikey can still be used for Public Key SSH
  - No check of the CRL
- Appliances do not check the Delta CRLs produced by the Microsoft CA server

Questions