



# The Long, Long Road to True Single Sign On at Fermilab

Al Lilianstrom and Dr. Olga Terlyga

NLIT 2018

May 22<sup>nd</sup>, 2018

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.

# 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](http://www.fnal.gov)

April 1, 2018



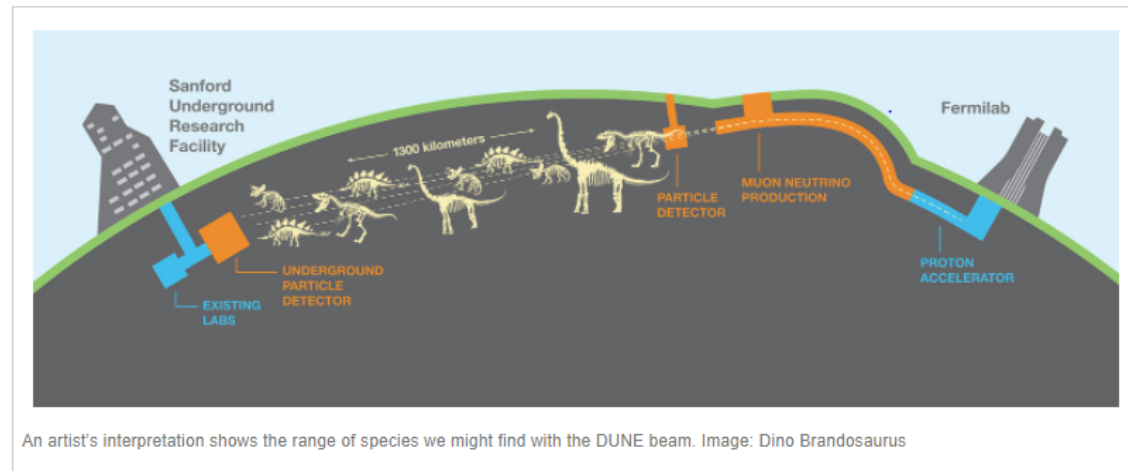
## We're also looking for dinosaurs

From neutrino oscillations to supernovas to proton decay, scientists working on the Deep Underground Neutrino Experiment pursue a broad set of research goals.

Now the DUNE collaboration might have found a completely new application: the search for gigantic dinosaur skeletons that might be hidden in Earth's crust.

"Most paleontologists believe that the Argentinosaurus was the largest animal ever to roam the Earth," said Professor Paul Sereno of the University of Chicago. "It probably weighed around 100 tons. But only a tiny fraction of animals ever get fossilized and discovered. It could well be there were dinosaurs that weighed 1,000 tons or more. With DUNE, we have the chance to find out."

DUNE will send a beam of neutrinos 800 miles straight through the Earth from Fermilab to particle detectors a mile underground at the Sanford Underground Research Facility. Most of the particles will go through rock and other material without leaving a trace, but occasionally a neutrino in the beam will interact with an atom and provide a signal that provides information about that atom.



# 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.

# The Long, Long Road

In 2012 Fermilab started down the road of single sign on for web applications. In 2018 the end of the road to true single sign on is in sight for all of our users – desktop or mobile, on premise or off. Join us as we describe the tools and techniques being used to provide this ease of access to our user community within the unique Fermilab environment.

FERMILAB-CONF-18-185-CD

# Has It Really Been That Long

2013



Managed by Fermi

**Authent  
at Fermi**

Al Lilianstro  
National Labo  
June 2014



Managed by Fer

**Federa**

Al Lilianstro  
National La  
May 2015





## Single Sign On at Fermilab A Year of Change

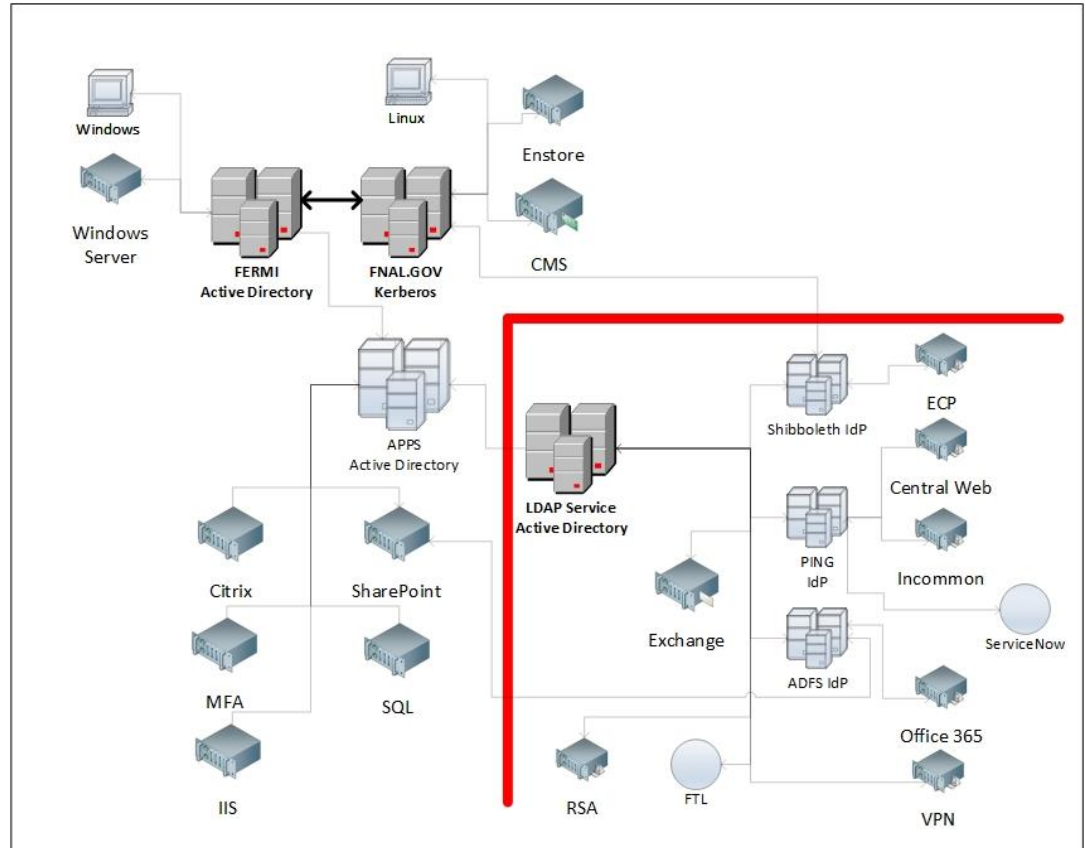
Al Lilianstrom and Dr. Olga Terlyga  
NLIT 2016  
May 2<sup>nd</sup>, 2016

# Over The Years

- Start with ADFS
  - SharePoint
  - Office 365
- Add Shibboleth
  - Apache web servers
- Replace Shibboleth with Ping Federate
  - Apache web servers
  - External SPs and IdPs
    - ServiceNow
    - InCommon
- Add Shibboleth
  - Enhanced Client or Proxy (ECP)
- Next...

# Central Authentication

- FERMI Domain
  - Windows systems
  - User accounts
- FNAL.GOV Kerberos Realm
  - Linux systems
  - User accounts
- LDAP Service
  - Application servers
  - User accounts
- Users are provisioned into all three services when a computer account is granted
  - Same username



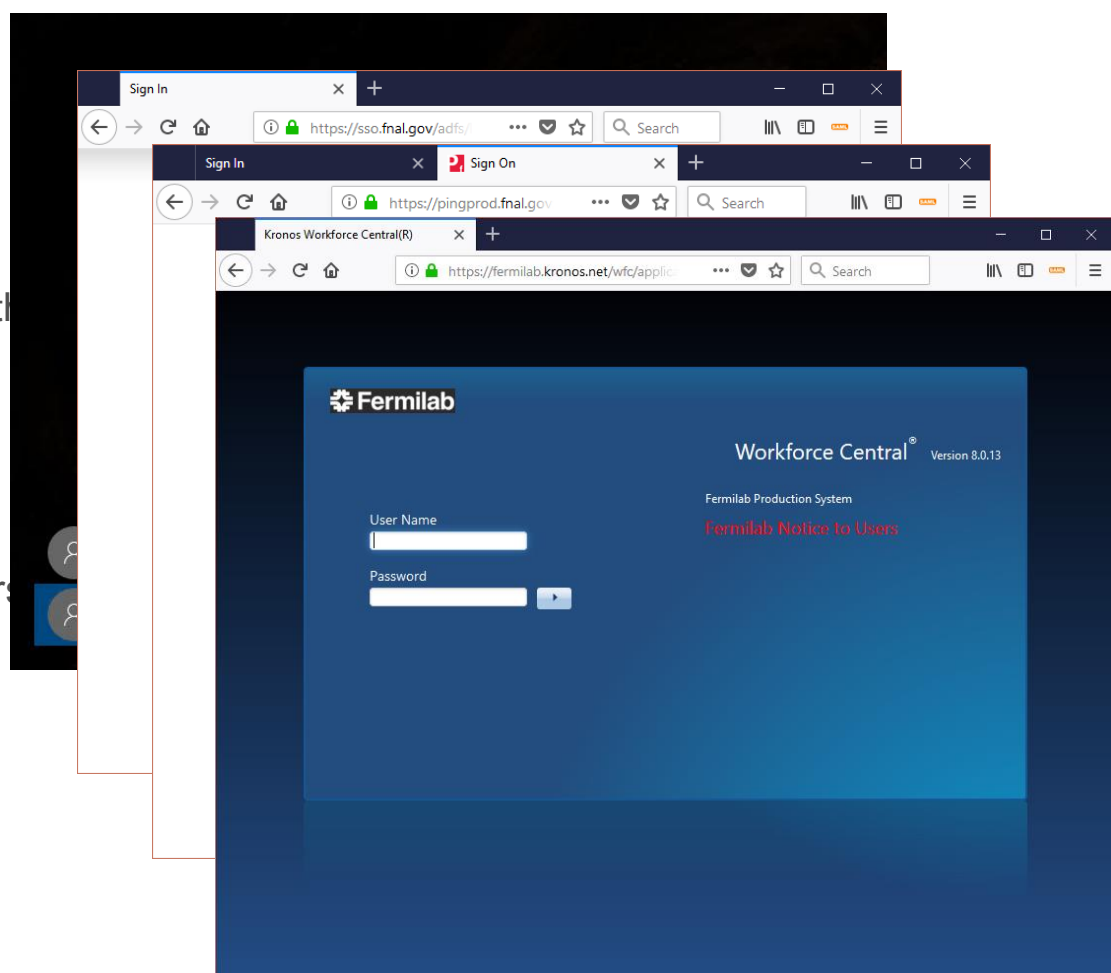


# User Experience

- Interactive
  - Strong Authentication
    - Kerberos (FNAL.GOV realm)
    - Active Directory (FERMI domain)
- Web Services
  - Not intended for interactive use
    - LDAP
    - ADFS
    - Ping Federate
- Our security policy prohibits the use of the FERMI domain and the FNAL.GOV realm for web services where the password is sent over the network between client and server

# User Experience

- Web Services
  - Username/Password
    - LDAP Service password – not the interactive login password
  - Multiple logons required
    - Desktop
    - ADFS Service Providers
    - Ping Federate Service Providers
    - LDAP Service Providers
- Our goals
  - One login for the desktop
  - Mobile device ease of use



# The Process

- Establish a relationship between Ping and ADFS
  - No impact or changes to Service Providers
    - PingFederate - 122
    - ADFS - 72
- Configure PingFederate
  - Kerberos Authentication
    - FERMI
    - FNAL.GOV
  - Certificate Authentication
    - CILogon
  - Username/Password

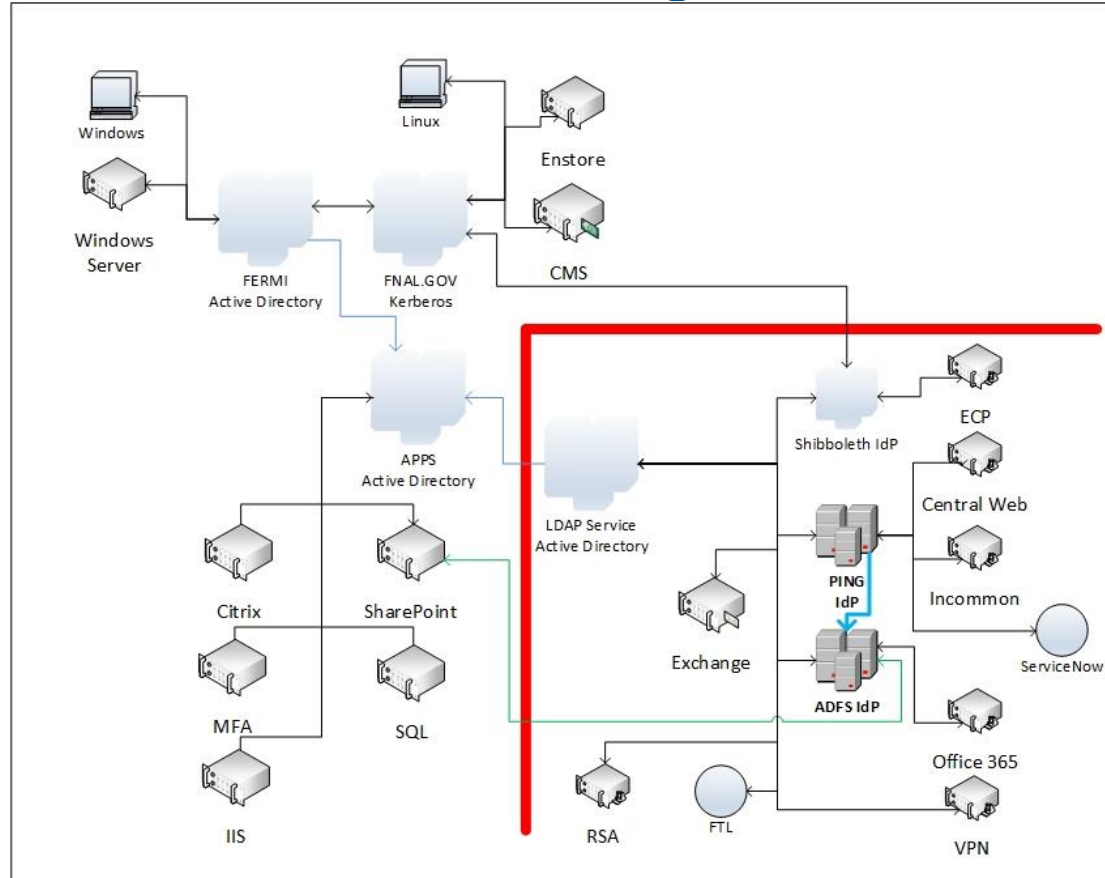
# ADFS

- Establish a IdP->SP relationship between PingFederate and ADFS
  - SAML
  - Use the SAML\_USER attribute coming from the PingFederate assertion to build a samAccountname and WindowsAccountname
    - `c:[Type == "SAML_USER"] => issue(Type = "http://schemas.microsoft.com/ws/2008/06/identity/claims/samaccountname", Value = c.Value);`
    - `c:[Type == "SAML_USER"] => issue(Type = "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Value = "SERVICES\" + c.Value);`
    - The ADFS SP rules use these values to build the proper assertion
- Now users accessing ADFS resources can choose to use the PingFederate service for authentication via a pull down menu

# ADFS

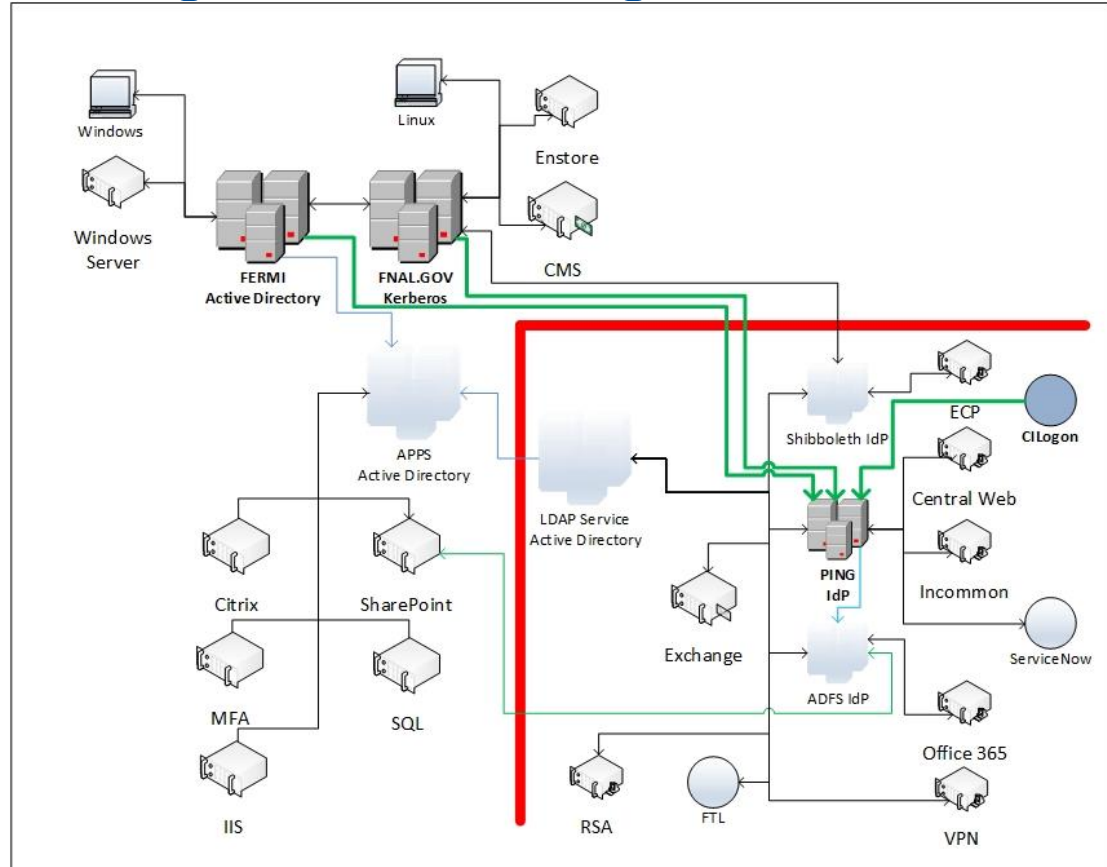


# Central Authentication – ADFS Changes



# Central Authentication – PingFederate Changes

- Kerberos adapters were added for FERMI and FNAL.GOV
- A certificate adapter was added for CILogon



# PingFederate Changes

- Composite Adapter
  - Combine
    - Kerberos
      - FERMI
      - FNAL.GOV
    - Certificate
    - Forms Based
      - Username/Password
- Goal was to start with Kerberos and fall through the adapters in order
  - FNAL.GOV Kerberos
  - FERMI Kerberos
  - Certificates
  - Username/Password



# Testing

- Each adapter worked individually
- Combined into a composite adapter
  - We had problems
  - Multiple adapter configurations were tried

# Problems

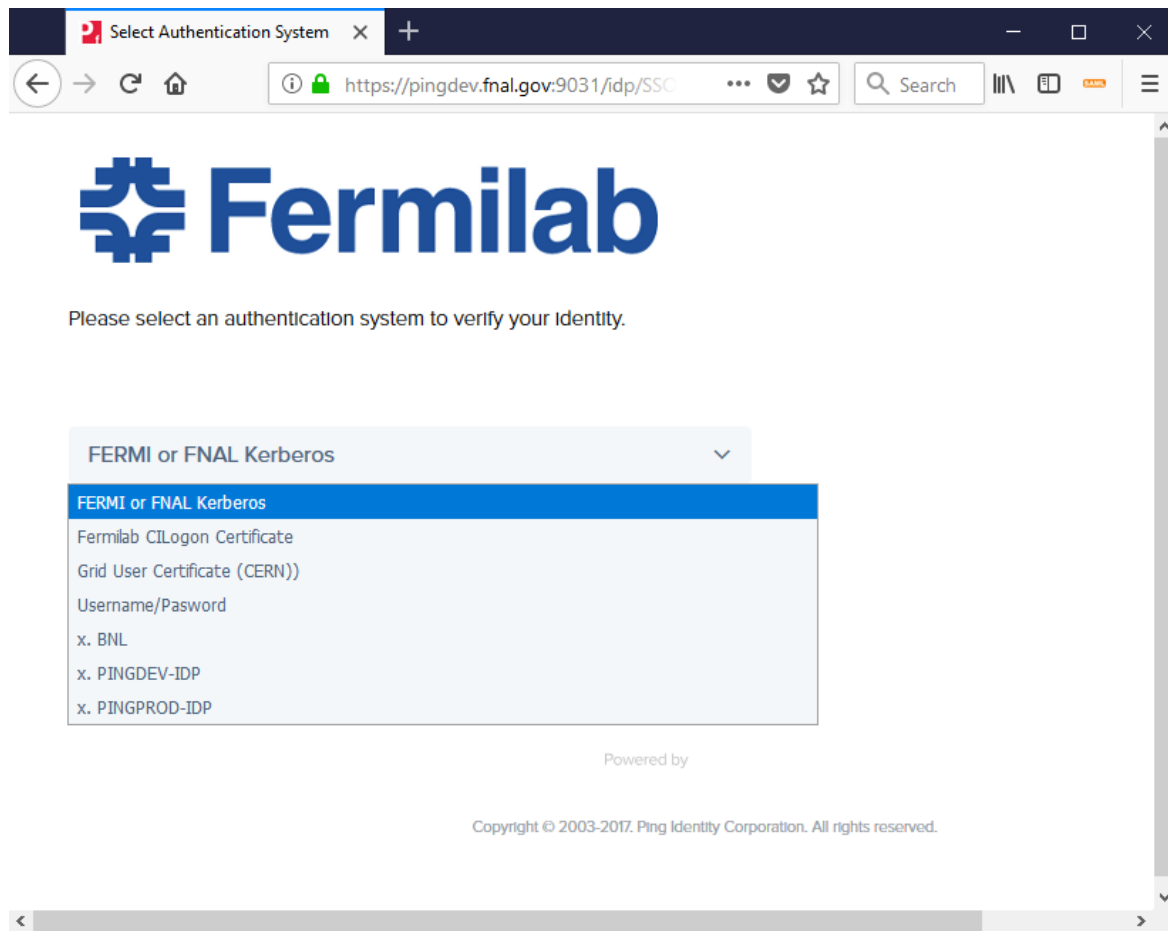
- Kerberos
  - Windows systems (FERMI Kerberos) would not fall through if FNAL.GOV was first
  - Linux / Mac systems (FNAL.GOV Kerberos) would hang on occasion
    - Cross Realm trust between FERMI and FNAL.GOV not working as expected
      - Errors in krb5.conf file?
- Certificates
  - Unusual pop ups
    - Dependent on client OS and browser
- Composite adapter combined with a pull down menu isn't sticky (bug)

# Solutions

- Fix krb5.conf
  - Authentication
  - Realm definitions
  - Take advantage of the cross realm trust
- New connection configuration
  - Pull down to select Authentication method
    - Kerberos (FERMI or FNAL.GOV)
      - Falls through to Username/Password
    - Certificates
      - Falls through to Username/Password
    - Username/Password

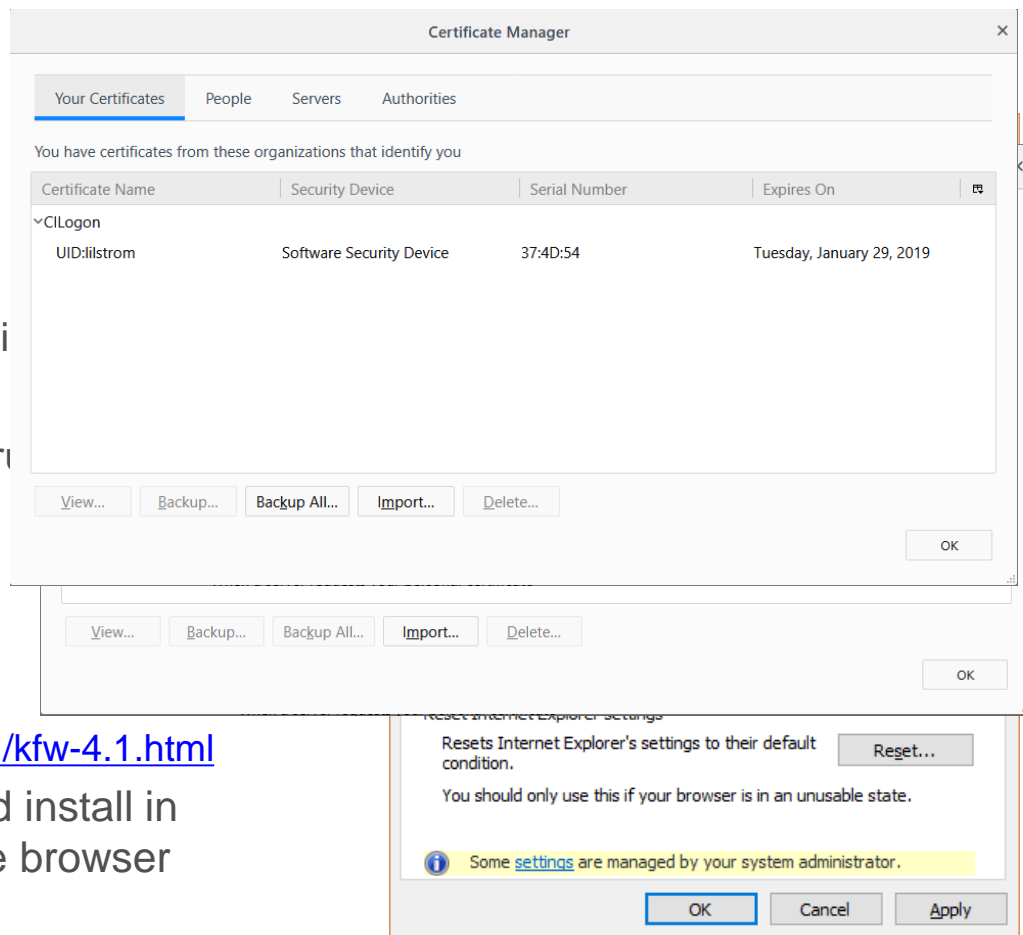
# Final Configuration

- Pull-down menu for each authentication method supported
  - Fall through to username/password supported
  - ‘Sticky’



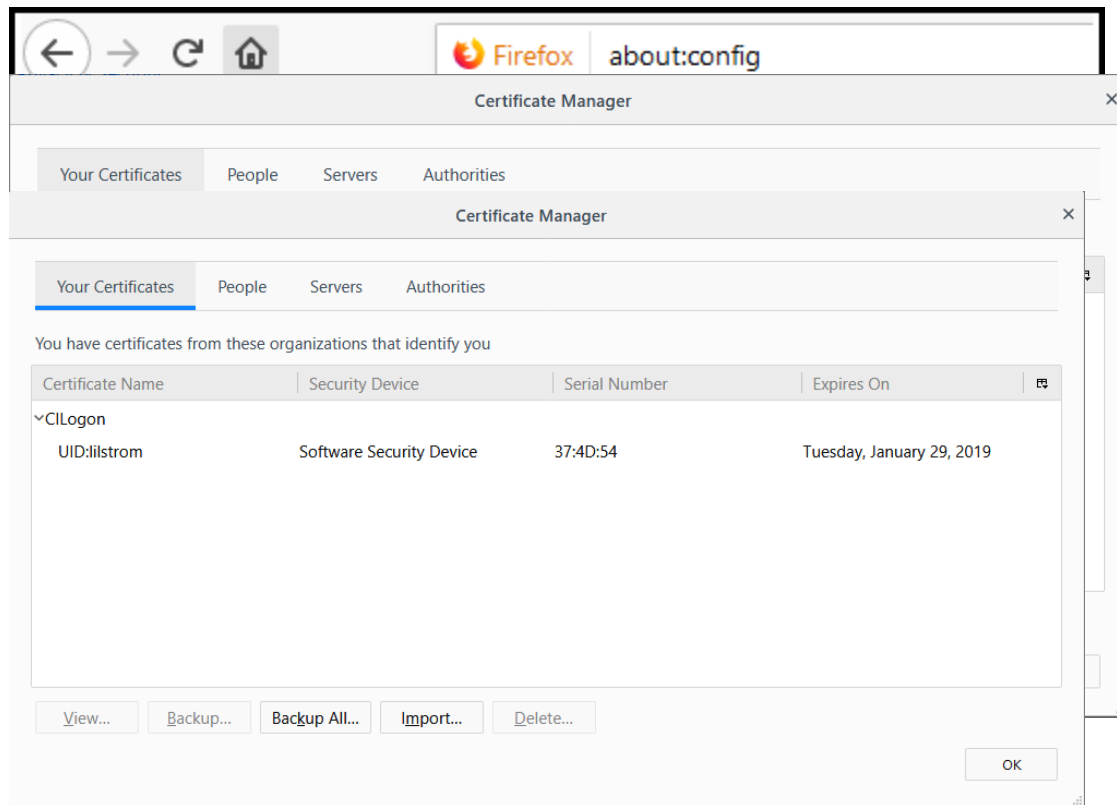
# Browser Configuration

- FERMI Windows Desktop
  - IE
    - Add IdP to Trusted Sites
    - Enable Integrated Windows Authentication
  - Firefox
    - Add IdP to network.negotiate-auth.trusteduris in about:config
- Standalone Windows Desktop
  - If using Kerberos – same as FERMI
    - MIT Kerberos for Windows
      - <http://web.mit.edu/kerberos/kfw-4.1/kfw-4.1.html>
  - If not – obtain CILogon certificate and install in the Personal Container for IE and the browser for Firefox



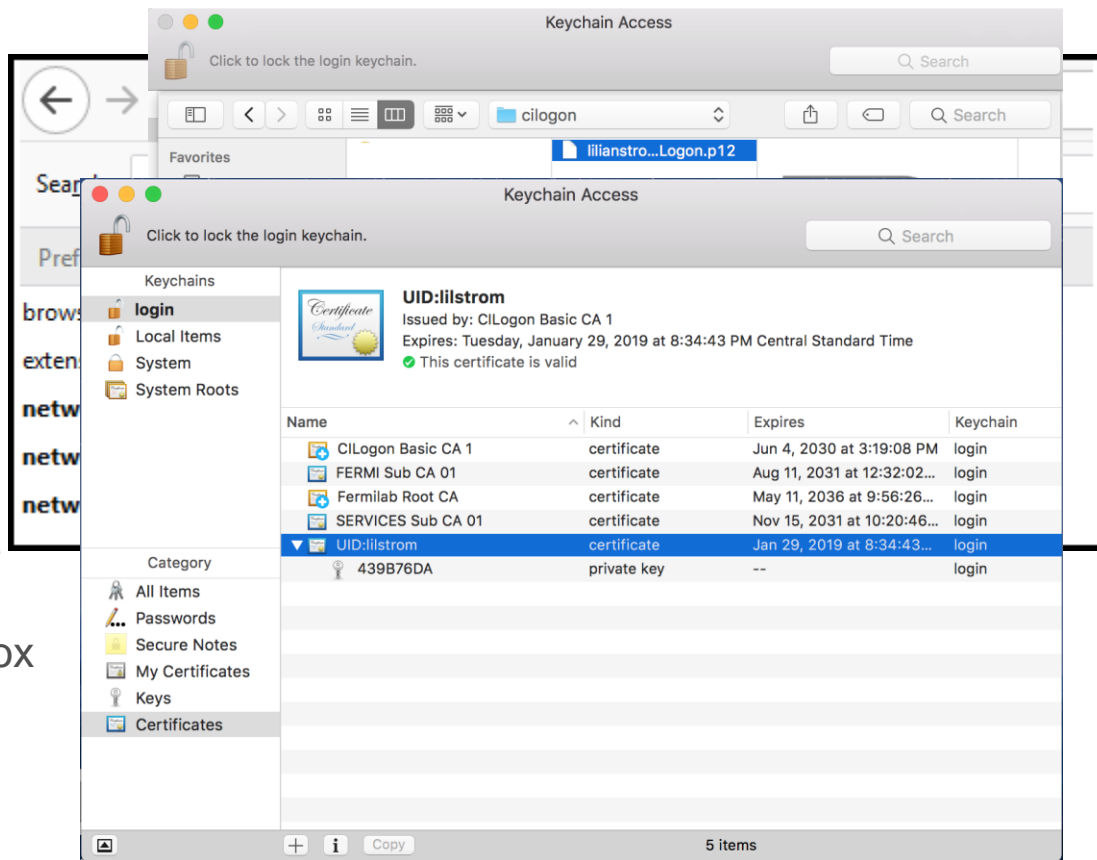
# Browser Configuration

- Linux Desktop
  - If using Kerberos
    - Updated krb5.conf
    - FireFox
      - Update about:config with IdP information
  - If not – obtain CILogon certificate and install in the browser



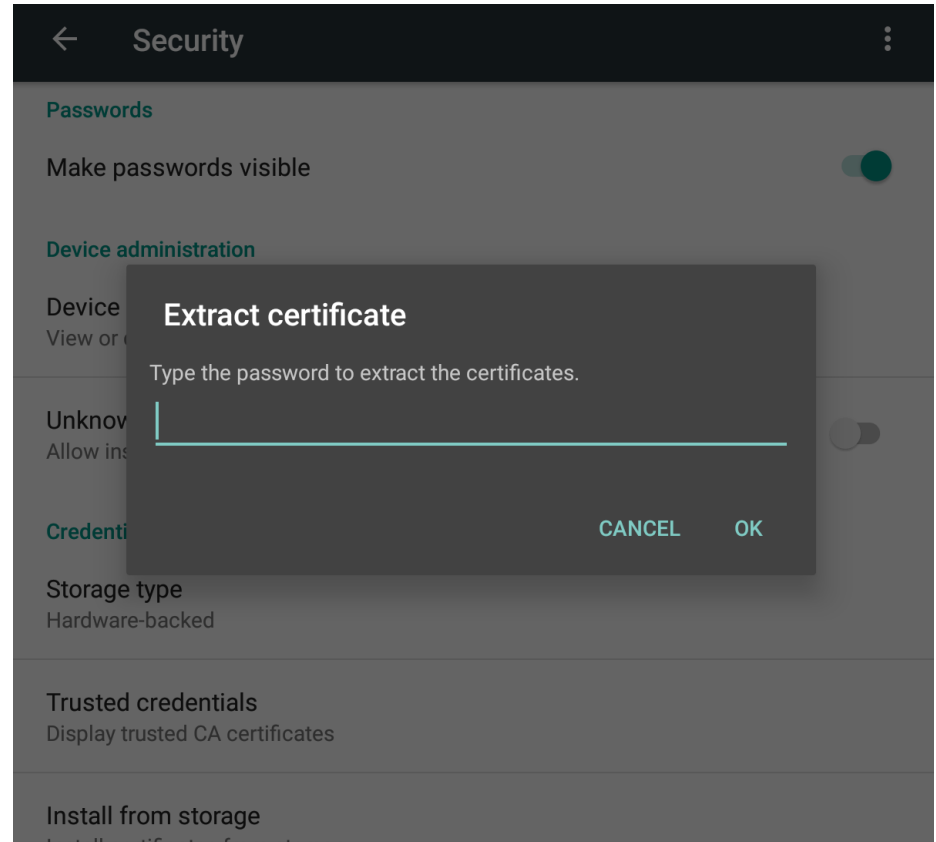
# Browser Configuration

- OSX Desktop
  - If using Kerberos
    - Updated krb5.conf
    - Firefox
      - Update about:config with IdP information
    - Safari works out of the box
  - If not – obtain CILogon certificate and install in the KeyChain for Safari or in the browser for Firefox



# Browser Configuration

- Mobile Device
  - Obtain CILogon certificate and install






# Usage

- Kerberos Authentication
  - FERMI Domain Windows Desktop
  - Standalone Windows Desktop with MIT Kerberos (FERMI or FNAL.GOV)
  - OSX or Linux Desktop with Kerberos (FERMI or FNAL.GOV)
    - Initial use – select authentication method
    - Subsequent uses - No prompts – direct to SP



Please select an authentication system to verify your Identity.

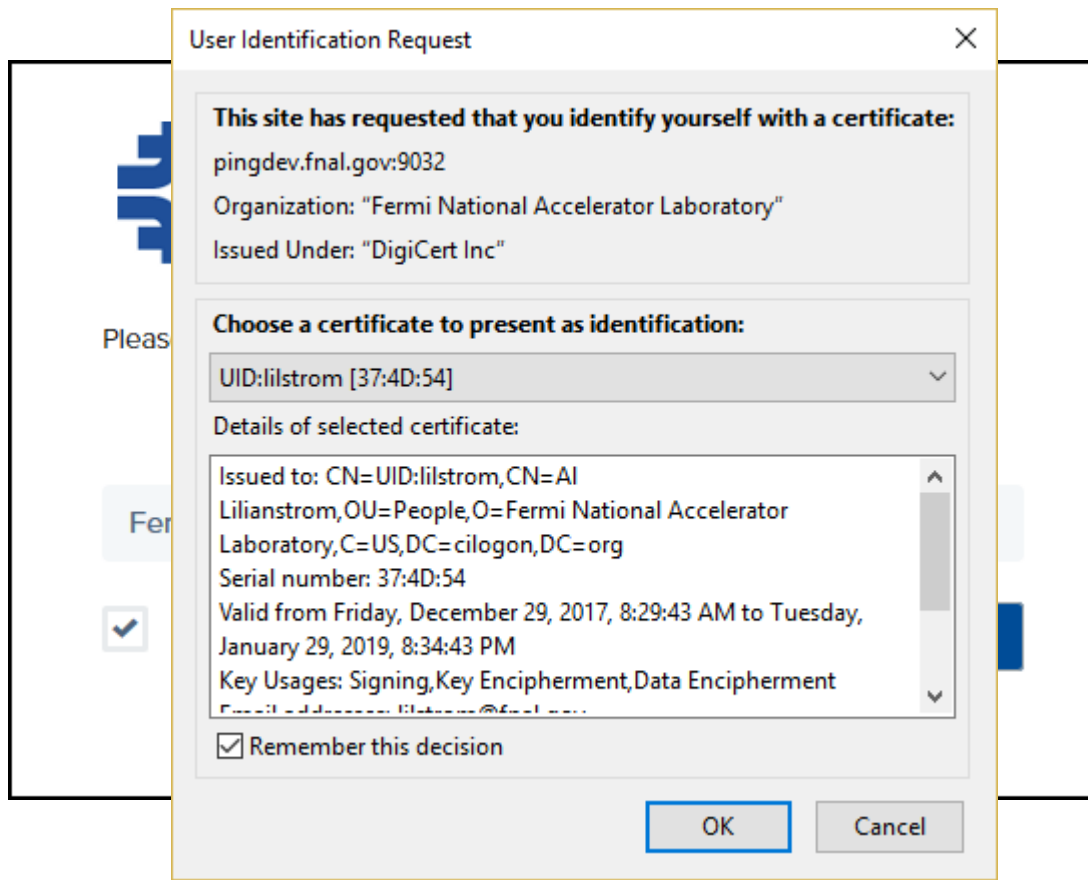
FERMI or FNAL Kerberos 

☒ Remember selection

[Continue](#)

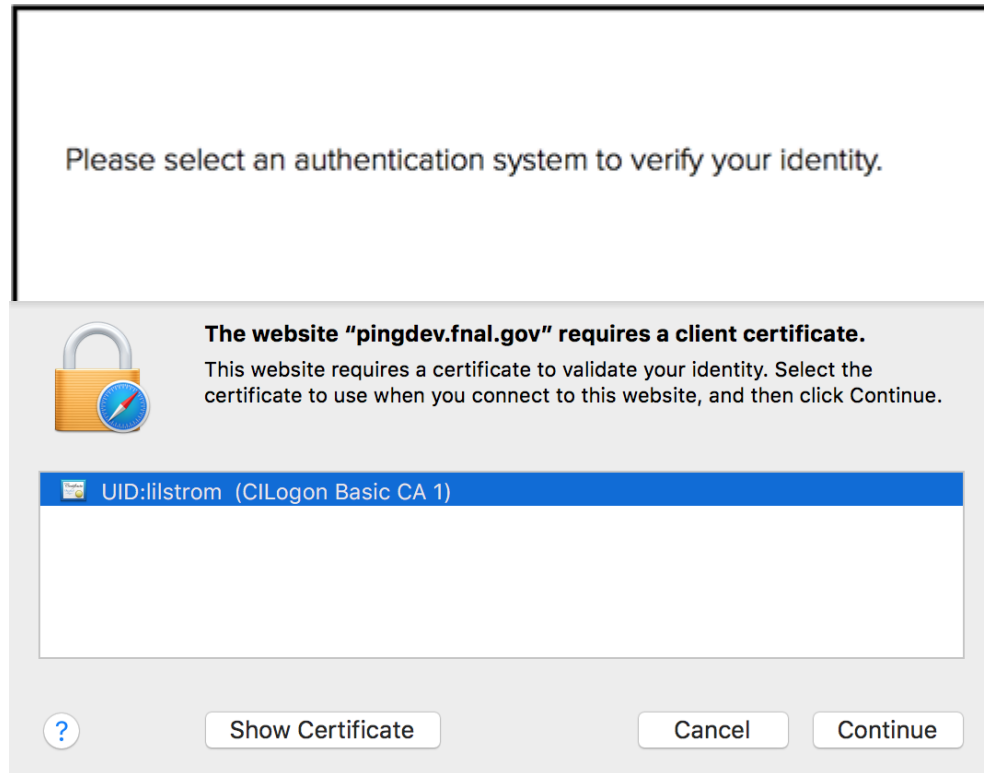
# Usage

- Desktop without Kerberos but with Certificate
  - Windows and Linux
    - Initial use – select authentication method, select certificate and go to SP
    - Subsequent uses - Select Certificate and go to SP



# Usage

- OSX
  - Initial use – select authentication method, select certificate, negotiate KeyChain access, and go to SP
  - Subsequent uses - Select certificate, negotiate KeyChain access, and go to SP



# Usage

- Mobile with Certificate
  - Initial use – Select certificate, select authentication method, and go to SP
  - Subsequent uses - Select Certificate and go to SP

**Choose certificate**

Please select an authentication system to verify your identity.

Fermilab CILogon Certificate

☒ Remember selection

Continue

# Usage

- No Kerberos or Certificate
  - All Platforms
    - Use Username / Password

A screenshot of the Fermilab login interface. At the top is the Fermilab logo, which consists of a blue stylized particle detector symbol followed by the word "Fermilab" in a bold, blue, sans-serif font. Below the logo, the text "Please enter your SERVICES user name and password." is centered. Underneath this text are two input fields: the first is labeled "USERNAME" and the second is labeled "PASSWORD". Both fields are light blue with a thin blue border. At the bottom right of the form is a blue button with the text "Sign On" in white.

# Questions