FERMILAB-SLIDES-18-102-CD

Fermilab

Managed by Fermi Research Alliance, LLC for the U.S. Department of Energy Office of Science

# Federation At Fermilab

Al Lilianstrom

National Laboratories Information Technology Summit

May 2015

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

- Since 1967, Fermilab has worked to answer fundamental questions and enhance our understanding of everything we see around us. As the United States' premier particle physics laboratory, we work on the world's most advanced particle accelerators and dig down to the smallest building blocks of matter.
- Fermilab collaborates with more than 20 countries on physics experiments based in the United States and elsewhere.
- Fermilab's 6,800-acre site is located in Batavia, Illinois, and is managed by the Fermi Research Alliance LLC for the U.S. Department of Energy Office of Science. FRA is a partnership of the University of Chicago and Universities Research Association Inc., a consortium of 86 research universities.

# Bison

# Terms

- ADFS – Active Directory Federation Services
  - https://technet.microsoft.com/en-us/windowsserver/dd448613.aspx
- COTS - Commercial Off The Shelf
- IdP – Identity Provider
- InCommon
  - https://www.incommon.org/
- LDAP – Lightweight Directory Access Protocol
  - http://en.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol
- SP – Service Provider
- SAML – Security Assertion Markup Language
  - http://saml.xml.org/about-saml
- Shibboleth
  - https://shibboleth.net/
- SSL – Security Sockets Layer
  - http://en.wikipedia.org/wiki/Transport_Layer_Security
- SSO – Single Sign On

# Abstract

- Fermilab is working to provide a seamless web for science and business applications by using federated identities from internal identity providers such as Active Directory Federation Services and Shibboleth and external identity providers such as InCommon Federation members and social identities such as Google.

- This talk will focus on the complexities of internal and external identities, open source and COTS identity providers, and open source and COTS applications and how we are working to make the user experience for authentication as simple and secure as possible.

# History

- 2008
  - Centrally managed LDAP service for web application authentication was brought online
  - Computer Security initiated push for web application owners to move from .htaccess files to LDAP over SSL
  - Not federation – just a single password
    - A big step in the right direction
- 2010
  - Fermilab hosted Shibboleth Installfest
  - 20+ attendees from Fermilab and several other institutions
  - Significant interest from all attendees

*Shibboleth 1.0 - 2003

# Crickets

# History

- 2013
  - ADFS IdP in Production
- 2014
  - ADFS SP
    - SharePoint 2013
    - Office 365
  - Shibboleth IdP in Production
    - On premise
    - Managed Service
  - Joined InCommon Federation
- 2015
  - CiLogon SP
    - Shibboleth Service

# Why Federate?

- Passwords
  - Same password as LDAP Service
    - Single Logon
- External identities
  - Social Media
    - Identity Proofing
  - Authoritative source
- Control of Information
- Platform Independent
  - OS/Application/etc
- Security Boundaries

# Why Federate?

- Identities
  - External identities
    - Business Partners
    - Social Media
      - Identity Proofing
        - How do you know who RadGenius@gmail.com really is?
    - Federation Members
    - Authoritative source
      - Termination
  - Authorization
    - Application Compatibility
      - Username
      - Email Address

# Why Federate?

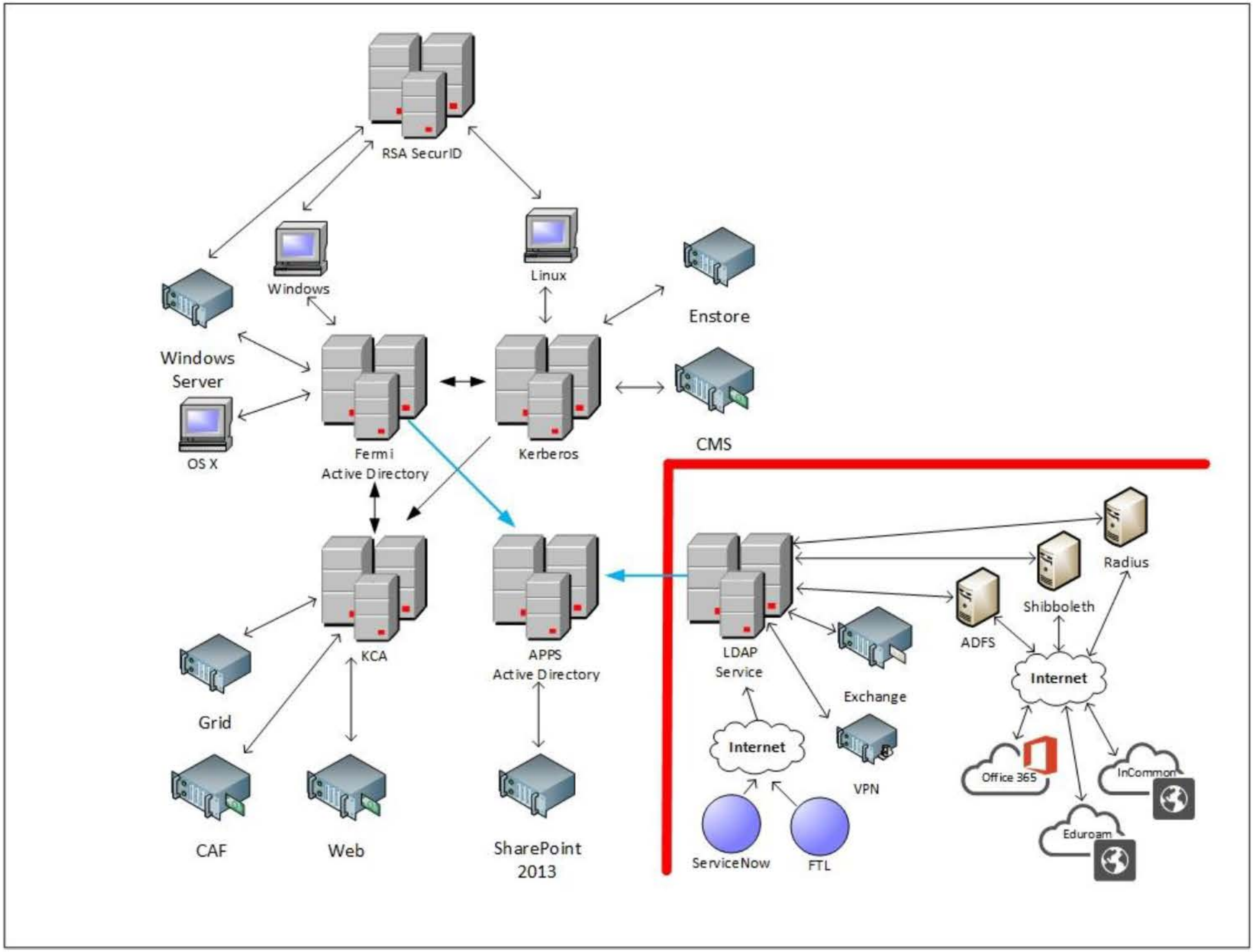
- Control of Information
  - Links not E-Mail
  - Authentication Source

- Platform Independent
  - Operating System
  - Application
    - SAML Support
      - SP
      - IdP
  - Client
    - Web Browser

# Security Boundaries

- Two types of logons at Fermilab
  - Interactive and Web
  - Password strength requirements are the same
    - Interactive
      - Logon to Linux or Windows
      - Remote Desktop
      - SSH
    - Web
      - SharePoint
      - Email
- Interactive logons are not used to access web services
- Web logons are not used for interactive access to computers
  - There is no direct connection between the services in the Interactive and Web environments

# Security Boundaries



# Security Boundaries

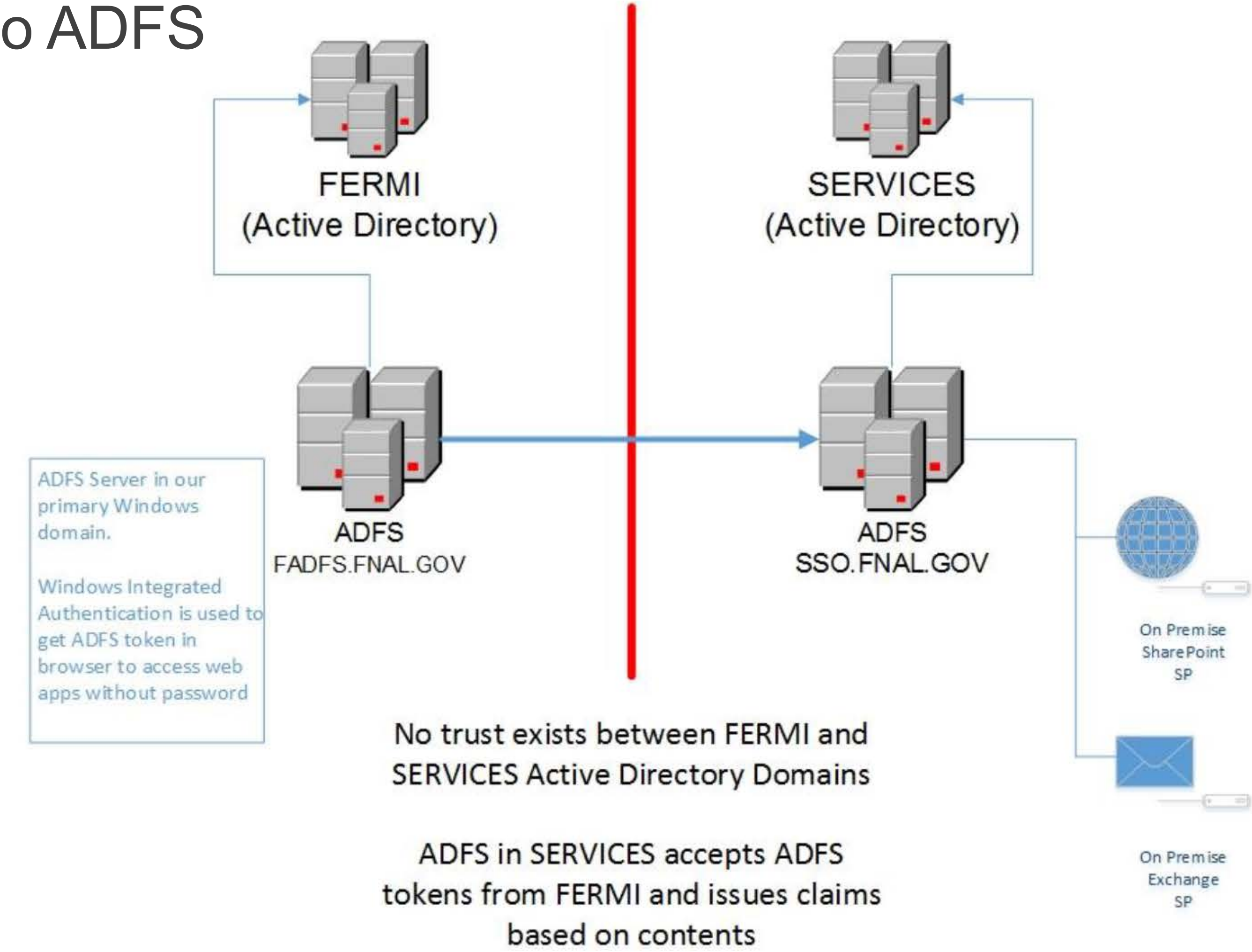
- Why?
  - Goal was to prevent compromised web credentials from gaining access to interactive systems
- As more services move to the web is this a valid concern?
- Some applications are designed around logon accounts being used to gain access to web services
  - Exchange
  - SharePoint
- Can Federation provide a true SSO environment?

# Security Boundaries

- ADFS
  - Windows Integrated Authentication
  - ADFS in Windows Logon Domain
    - IdP as a RP to primary ADFS IdP
  - Logon credentials used to access web applications
    - Logon credentials are never presented to the web application
    - No passwords on the wire
      - Ever
  - Non-Windows clients can kinit against the Windows Domain and use the applications in the same manner*

# Security Boundary

- ADFS to ADFS



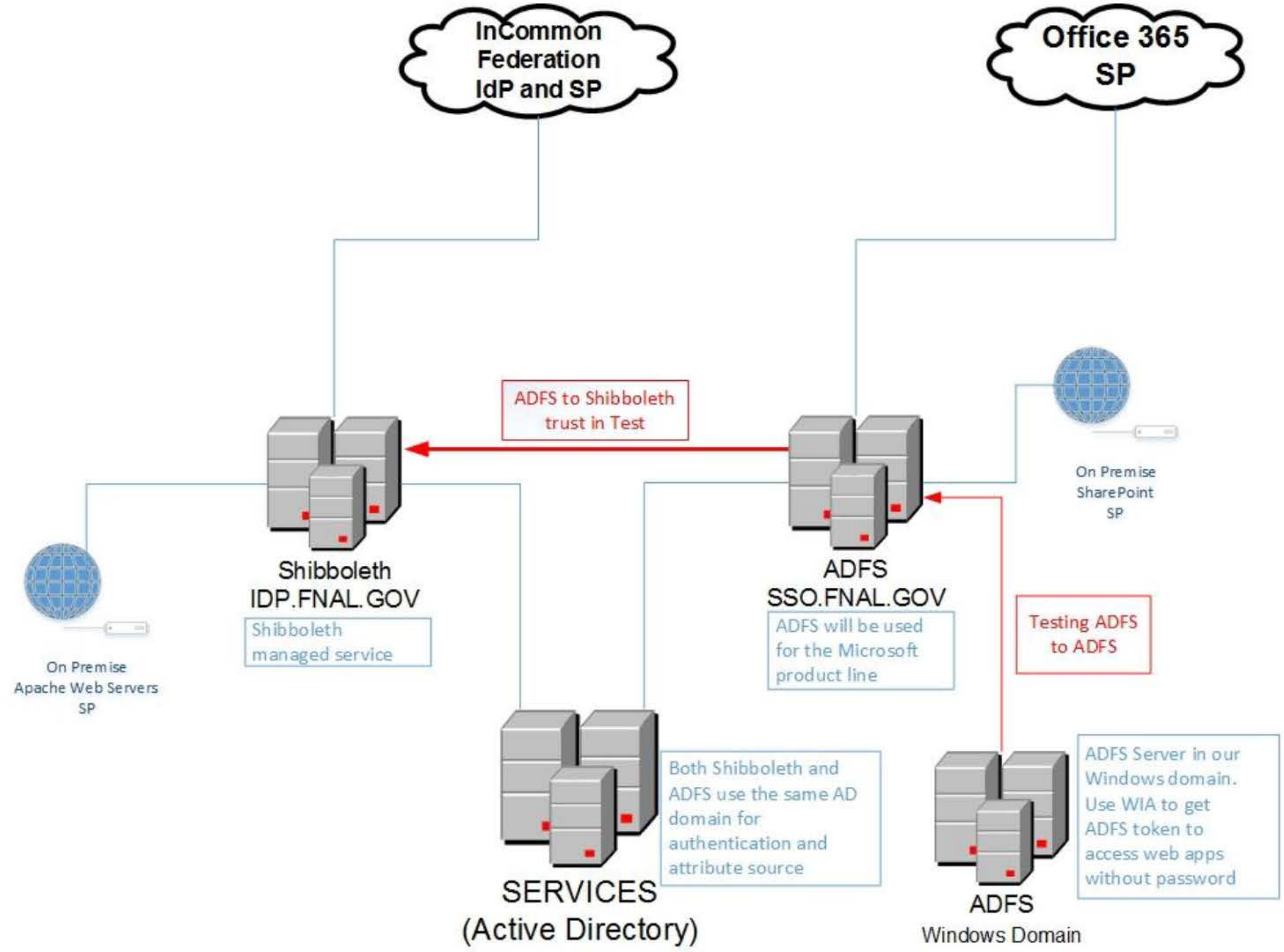
ADFS Server in our primary Windows domain.

Windows Integrated Authentication is used to get ADFS token in browser to access web apps without password

No trust exists between FERMI and SERVICES Active Directory Domains

ADFS in SERVICES accepts ADFS tokens from FERMI and issues claims based on contents

# Federation Service Today



Shibboleth managed service

ADFS will be used for the Microsoft product line

Both Shibboleth and ADFS use the same AD domain for authentication and attribute source

ADFS Server in our Windows domain. Use WIA to get ADFS token to access web apps without password

# Federation Service Today

- Hybrid Solution
  - ADFS
    - Microsoft stack
      - SharePoint
      - Office 365
  - Shibboleth
    - Everything else ☺
      - InCommon
      - CiLogon
      - Central Web Services
      - Service Now
      - Apache Based Applications
      - Social Connections

# Hybrid Solution

- Issues
  - Usability
    - Two IdPs
      - IdP to IdP Trust
  - Support
    - Managed Service Issues
  - Compatibility
    - Claims
      - Formats

# Hybrid Solution

- Why not just use one?
- ADFS
  - Microsoft Documentation
  - Microsoft Applications
  - Open Source Applications
    - Evil Empire ☺
  - PowerShell
  - Internal Support
    - System Configuration
      - Hardware
      - Software
  - Quirks
  - ADFS is an excellent choice for a Windows shop

# Hybrid Solution

- Shibboleth
  - Microsoft Applications
    - Supported but …
  - Open Source Applications
  - Documentation
  - Product Support
    - Paid
      - https://shibboleth.net/community/consultants.html
    - Free
      - Not always friendly
  - Internal Support
    - System Configuration
      - Hardware
      - Software

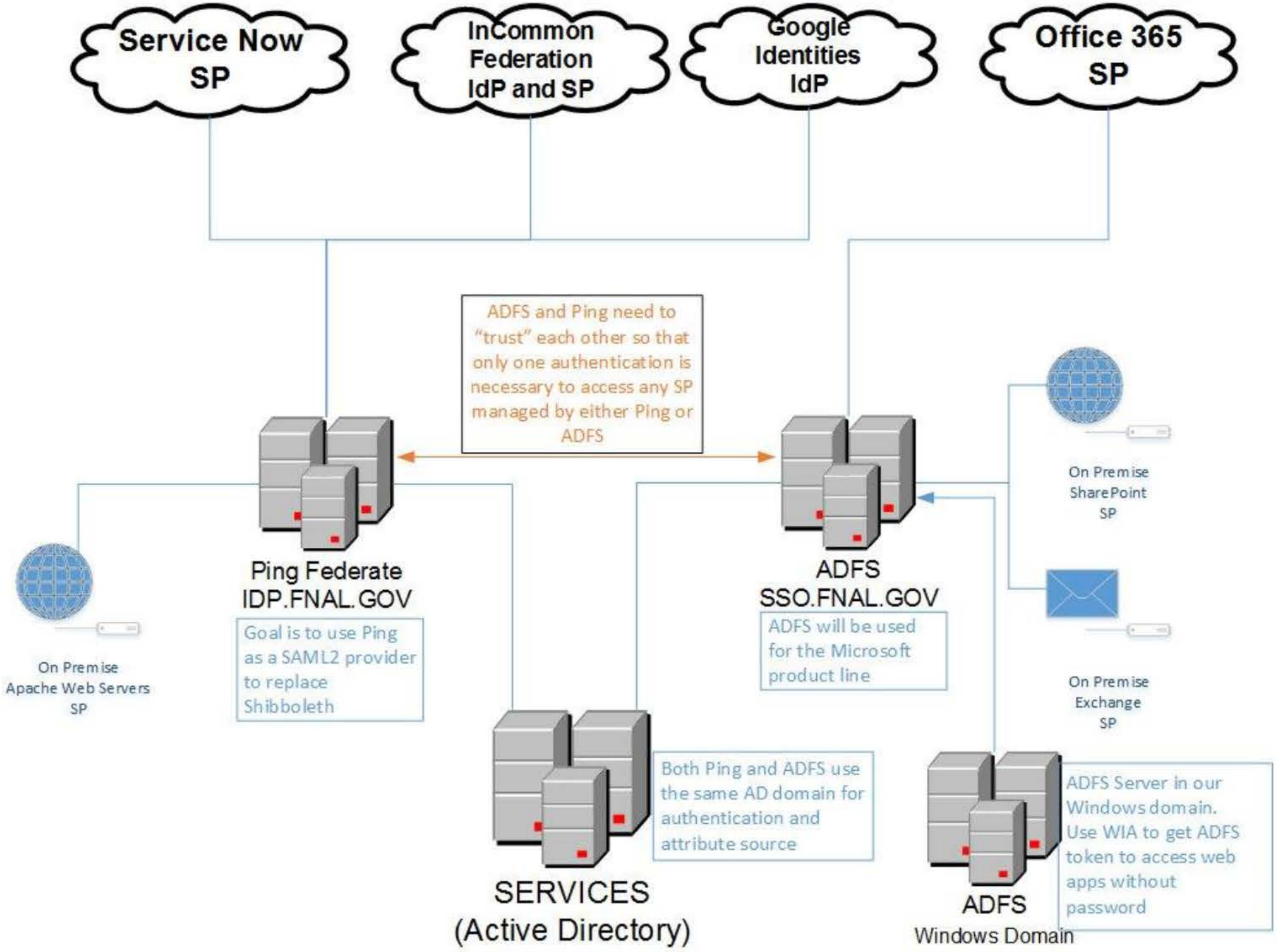
# Changing the Solution

- Federation is starting to gain acceptance at Fermilab
  - Multiple SPs testing
    - Central web services
    - Content Management
    - Cloud SaaS
- Issues with current solution
  - Support
  - Reliability
- Need a robust supported solution
  - Internal Support
  - Vendor
  - Third-party

# Federation Phase Three

- Shibboleth out, Ping Federate in
    - Standards Compliant
    - Industry leader
    - Excellent support
    - In use in the DOE complex
    - Mobile device integration
    - Not without issues
        - Configuration
        - Metadata
            - Import
            - Export
        - IdP Trust

# Federation Service – Planned



ADFS and Ping need to "trust" each other so that only one authentication is necessary to access any SP managed by either Ping or ADFS

Goal is to use Ping as a SAML2 provider to replace Shibboleth

ADFS will be used for the Microsoft product line

Both Ping and ADFS use the same AD domain for authentication and attribute source

ADFS Server in our Windows domain. Use WIA to get ADFS token to access web apps without password

# Federation Phase Four

- Simplify ADFS
  - As part of “upgrade” to ADFS v3
  - Move from SQL Server to Windows Integrated Database
- More redundancy
  - Data Centers
    - Ping Federate
    - ADFS
    - Domain Controllers
    - Cloud

# Federation Service – Goals

- True SSO for Windows Users
  - Domain Members
- True SSO for Linux and OSX Users
  - Kerberos Login Required
- Forms Based SSO
  - All other
- Mobile Device Support
  - Improve ease of use

# Lessons Learned

- COTS
  - Features
  - Support
- Open Source
  - Support Issues
- Managed Service
  - Vendor Response
- Standards
  - Support

# Lessons Learned

- Evaluate the market
  - Products are constantly evolving
- Don’t be afraid to change
  - Results can be worth the pain

- Questions?

- Contact Information
  - Al Lilianstrom
  - lilstrom@fnal.gov