



---

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

---

## KCA Futures

Al Lilianstrom

September 9<sup>th</sup>, 2015

# Agenda

---

- What is a KCA?
- History of the KCA at Fermilab
- Current Status of the KCA
- The Future of the KCA at Fermilab

# This Meeting

---

- Community outreach
- Service Providers
  - Accepting KCA certificates
    - Web sites
    - Other services

# What is the KCA?

---

- Kerberos Certificate Authority
  - Requires the use of Kerberos Authentication to issue a short lifetime x.509 certificate for user identification
    - FNAL.GOV Realm
    - FERMI Windows Domain
  - Certificates issued have a lifetime of 7 days
  - Limited usage
    - Client identification
      - Not for email or code signing

# History of the KCA at Fermilab

---

- 2003
  - Initial implementation on Solaris
  - Based on code from the University of Michigan
- 2009
  - Application ported to Windows Server 2003 and integrated with the Fermi domain
- 2009
  - Hardware Security Module (HSM) installed
- 2015
  - Hardware upgrade
  - OS upgrade to Windows Server 2008

# The Status of the KCA Service Today

- Production KCA Service
  - Latest release of the KCA code
  - Issuing SHA1 signed certificates

Field	Value
Version	V3
Serial number	03 67 de a1
Signature algorithm	sha1RSA
Signature hash algorithm	sha1
Issuer	Kerberized CA HSM, Certificat...
Valid from	Monday, September 7, 2015 5...
Valid to	Tuesday, September 15, 2015...
Subject	UID: , Pe...

- Test KCA Service
  - Latest release of the KCA code
  - Issuing SHA2 signed certificates

Field	Value
Version	V3
Serial number	27 b4 2d 15
Signature algorithm	sha512RSA
Signature hash algorithm	sha512
Issuer	Kerberized CA HSM, Certificat...
Valid from	Monday, September 7, 2015 1...
Valid to	Tuesday, September 15, 2015...
Subject	UID: , Pe...

- SHA2 signed certificates required for TAGPMA accreditation
- **SHA2 signed certificates are coming later this year to the Production KCA Service**

## KCA Futures – Short Term

---

- If your service accepts KCA certificates **TEST** with SHA2 signed certs
  - SHA1 scheduled for deprecation in November

If your service does not accept SHA2 certificates when the KCA Service moves to SHA2 your service will stop functioning

# KCA Futures – Short Term

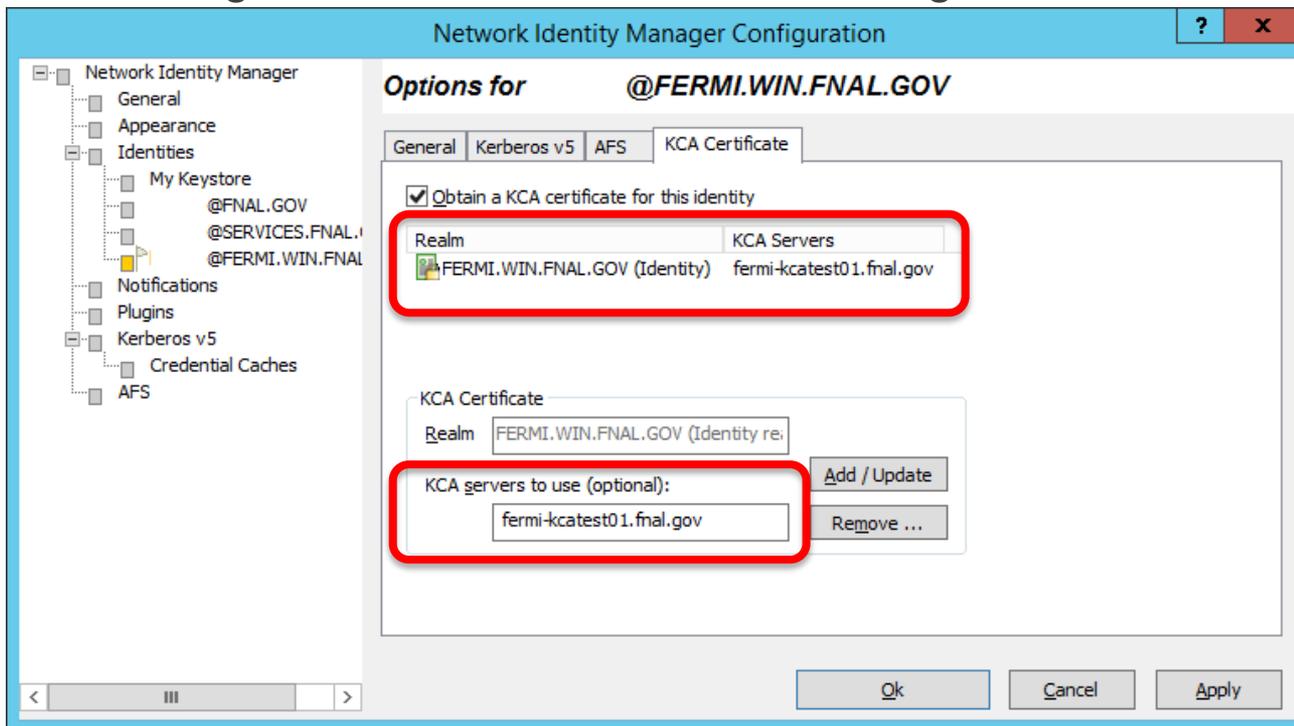
## – Test Server Certificates

- Linux/OSX

- getcert –t

- Windows

- Change server to fermi-kcatest01.fnal.gov inside NetID Manager



# KCA Futures – Long Term

---

- Budget related discussion led to the following statement from our support vendor (Secure Endpoints):

“What I am saying is that it is probably time to look for an alternative to the KCA. We need to replace the HSMs, the kx509 protocol, and the crypto library. “
- Fermi is the only Secure Endpoints customer using KCA/HSM
  - By the end of calendar 2015 we may be the only Secure Endpoints customer...
- So where do we go?

# KCA Futures – Long Term

---

- KCA users
  - Web sites
  - Grid
  - Other?
- Alternatives
  - Federated Identity/Single Sign On
  - CiLogon Certificate Authority
  - Stand up another internal Certificate Authority?
- Assuming everything works as expected decommission KCA service at the end of FY16

# Federated Identity

---

- Development and Production instances of Ping Federate have been stood up
  - Now live
- Connected to InCommon and CiLogon
- Next
  - Service Providers
    - Central Web
  - Identity Providers
    - OpenID
    - OAuth

# CiLogon

---

- <https://cilogon.org/>
  - Allows users to authenticate with their home organization and obtain a certificate for secure access to CyberInfrastructure
    - <http://www.nsf.gov/div/index.jsp?div=ACI>
  - Longer lifetime – up to 13 months
- Certificates can be obtained via web browser or command line
  - ECP Support
    - Enhanced Client or Proxy
      - SAML v.2.0 profile which allows for the exchange of SAML attributes outside the context of a web browser. (command line, thick client, etc)
    - <http://www.cilogon.org/ecp>
    - Ping Federate does not support ECP at this time

# CiLogon

---

- Test ECP Server is online
  - <https://idpdev-ecp.fnal.gov>
    - ECP only
    - SERVICES credentials
      - username/password

# Internal Certificate Authority

---

- Microsoft CA
  - No experience with this product
  - Implementation is part of the Authentication 3 year plan
    - Delayed to to resource issues
    - Necessary for another internal project
- EJBCA
  - No experience or resources available

# Recommendations

---

- Web Sites
  - Test with SHA2 signed certificates to be ready for the November deprecation of SHA1
  - Move to the central federated identity service
  - If you must use certificates investigate the use of CiLogon certificates with your service
  
- Non-web services
  - Test with SHA2 signed certificates to be ready for the November deprecation of SHA1
  - Investigate the use of CiLogon certificates with your service

# Questions

---

Al Lilianstrom

Group Leader, Authentication Services Group

[lilstrom@fnal.gov](mailto:lilstrom@fnal.gov)

x2028