

Kerberos Authentication at Fermilab

Keith Chadwick

Fermilab Grid Department

chadwick@fnal.gov

Work supported by the U.S. Department of Energy under contract No. DE-AC02-07CH11359

Outline

- Hierarchy of Authentication Methods
- Components of the Authentication and Authorization Infrastructure
- User Registration Workflow
- Fermilab Virtual Organization
- People vs. Robot Credentials
- Fermilab KCA vs. DOEgrids CA
- Some Statistics
- Other Authentication and Authorization Infrastructure at Fermilab
- Plans for the Future

Fermilab Supports a Hierarchy of Authentication Methods

Strong Authentication:

- MIT Kerberos
- Active Directory (Windows Kerberos)

LDAP:

- Services "Domain"

Local Authentication:

- Access to "desktops" that do not offer services.

Legacy Authentication:

- Access to services that don't support strong authentication or LDAP (services domain).
- Typically these are various business applications.

Components

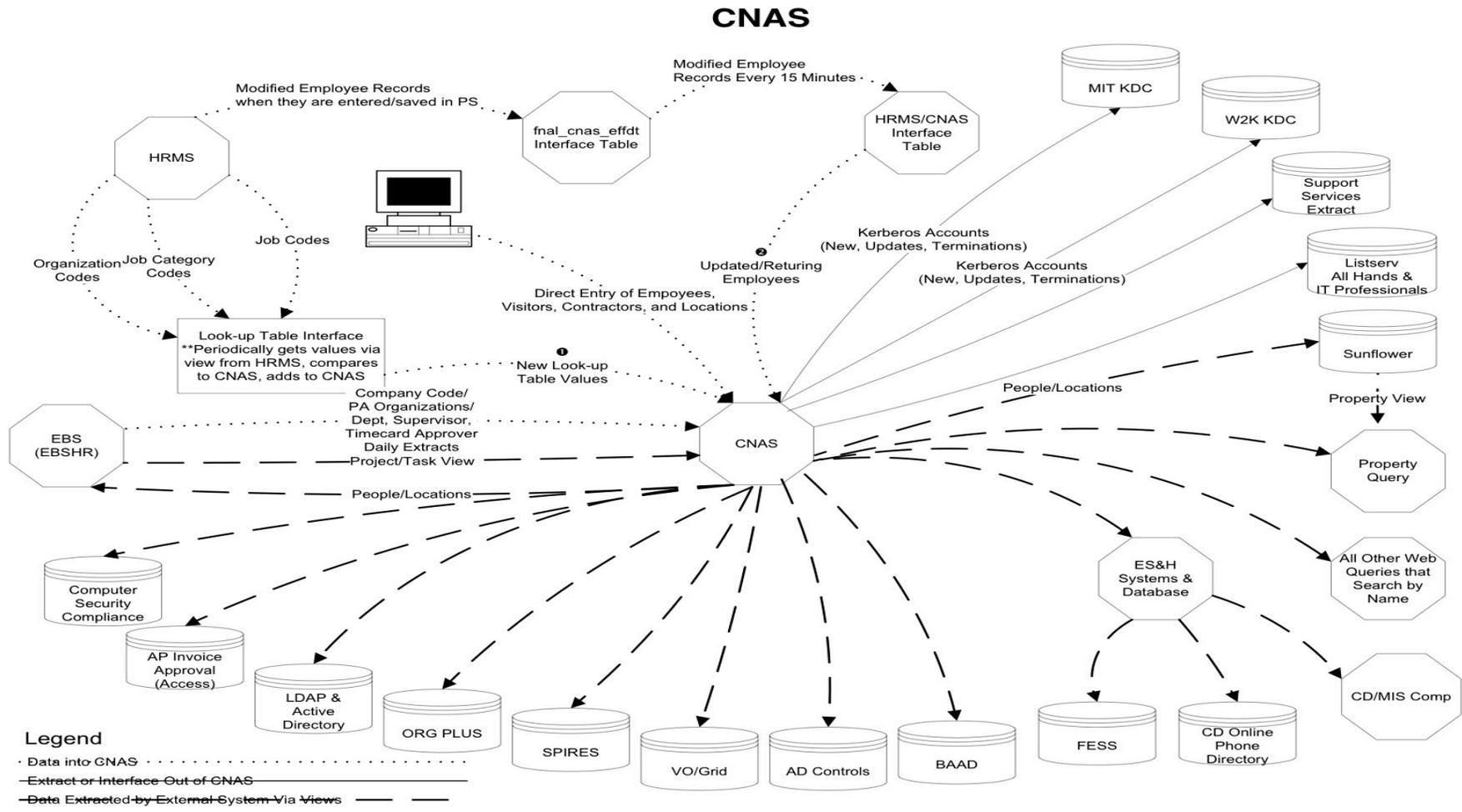
- Central Name and Address Service (CNAS)
- MIT Kerberos Domain Controller (MIT KDC)
- Active Directory Windows Domain Controller (AD KDC)
- Kerberos Certificate Authority (KCA)
- Virtual Organization Membership Registration Service (VOMRS)
- Virtual Organization Management Service (VOMS)
- Grid User Mapping Service (GUMS)
- Site AuthorizAtion (SAZ) Service
- Globus Gatekeepers and gLExec
- A cast of 1,000s of Worker Nodes

Centralized Name and Address System (CNAS)

CNAS is the repository for the identity information for all Fermilab “badged” personnel:

- Full, Part-Time and “Term” Employees,
- Visitors (Experimenters),
- [Sub]Contractors,
- Summer Students,
- On-call,
- Etc.

CNAS Interconnections



Registration Workflow – Step 1

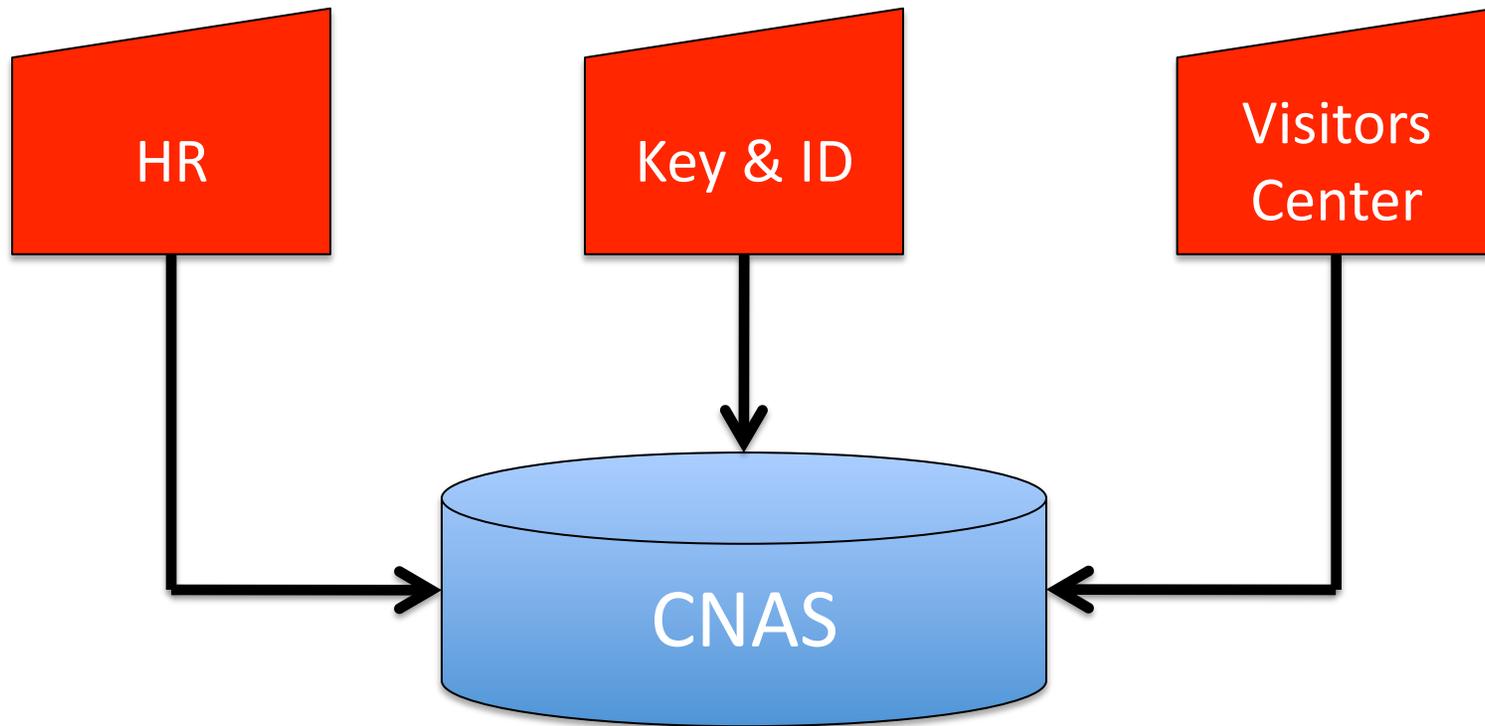
People are registered into CNAS through three avenues:

- Data entry by Fermilab human resources personnel as employees are on boarded,
- Data entry by the Fermilab key and id office as individuals are issued keys and official laboratory identification,
- Data entry by the Fermilab visitor office as experimental users (visitors) complete the registration process.

This information is (>99% of the time) captured during a face-to-face interview.

- There is a mechanism to get the necessary information into CNAS in the (rare) event that an individual is unable to travel to Fermilab.

Workflow - Diagram 1



Registration Workflow – Step 2

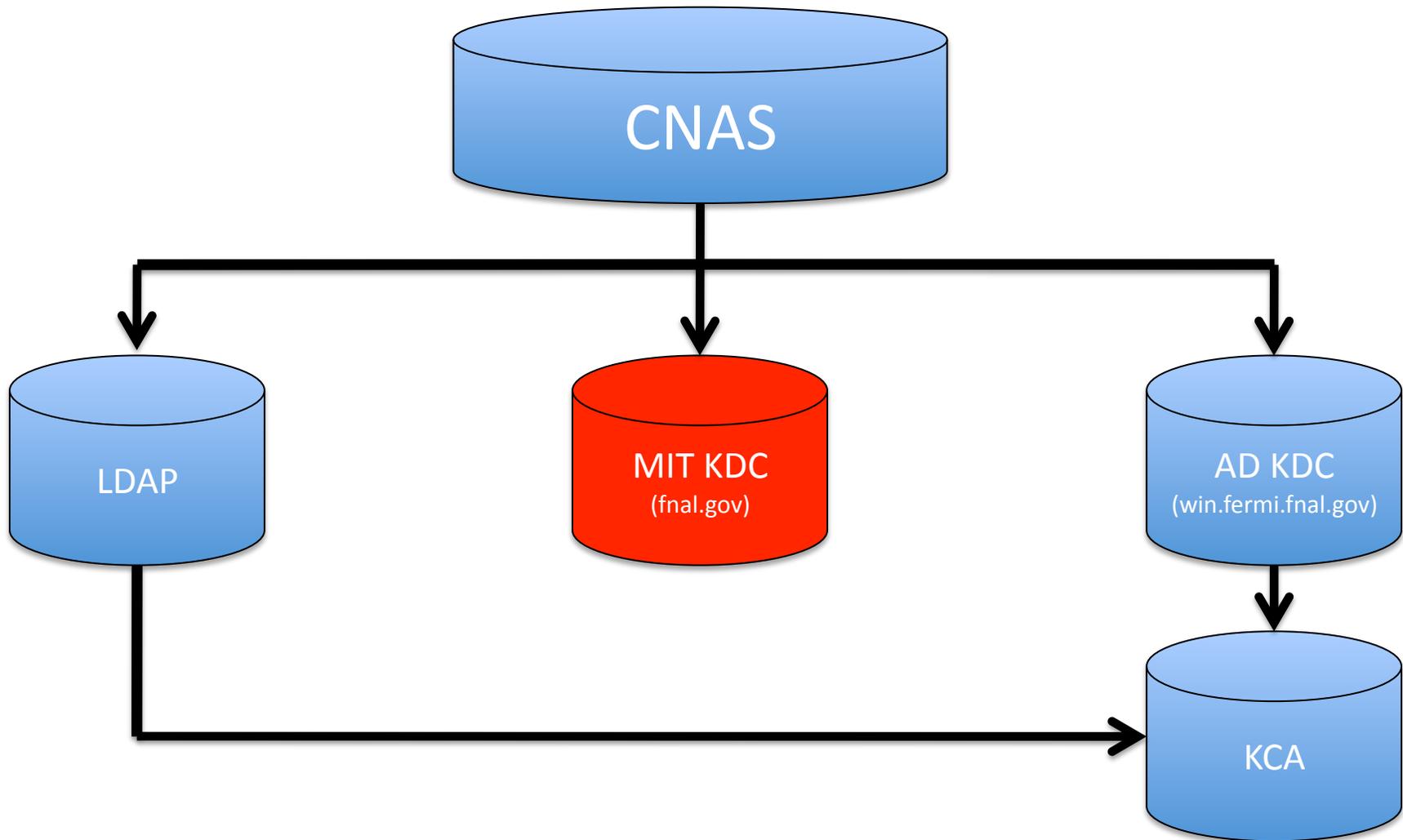
When an individual requests a computer account, the previously registered information in CNAS provides the basis for the account creation by the Fermilab service desk.

Once the account is authorized by the appropriate line or experiment management,

- The account information is propagated into the Fermilab ldap database,
- A Kerberos account is created in the Fermilab “MIT” Kerberos Domain Controller (KDC),
- A Windows account is created in the Fermilab “Active Directory” Kerberos Domain Controller (AD).

Information from ldap and the AD KCD is combined and the necessary DNS are created in the Fermilab Kerberos Certificate Authority (KCA).

Workflow - Diagram 2



Registration Workflow – Step 3

Once the DN information is in the Fermilab KCA,

- Scripts automatically “publish” the list of valid DNs (typically three times every hour).

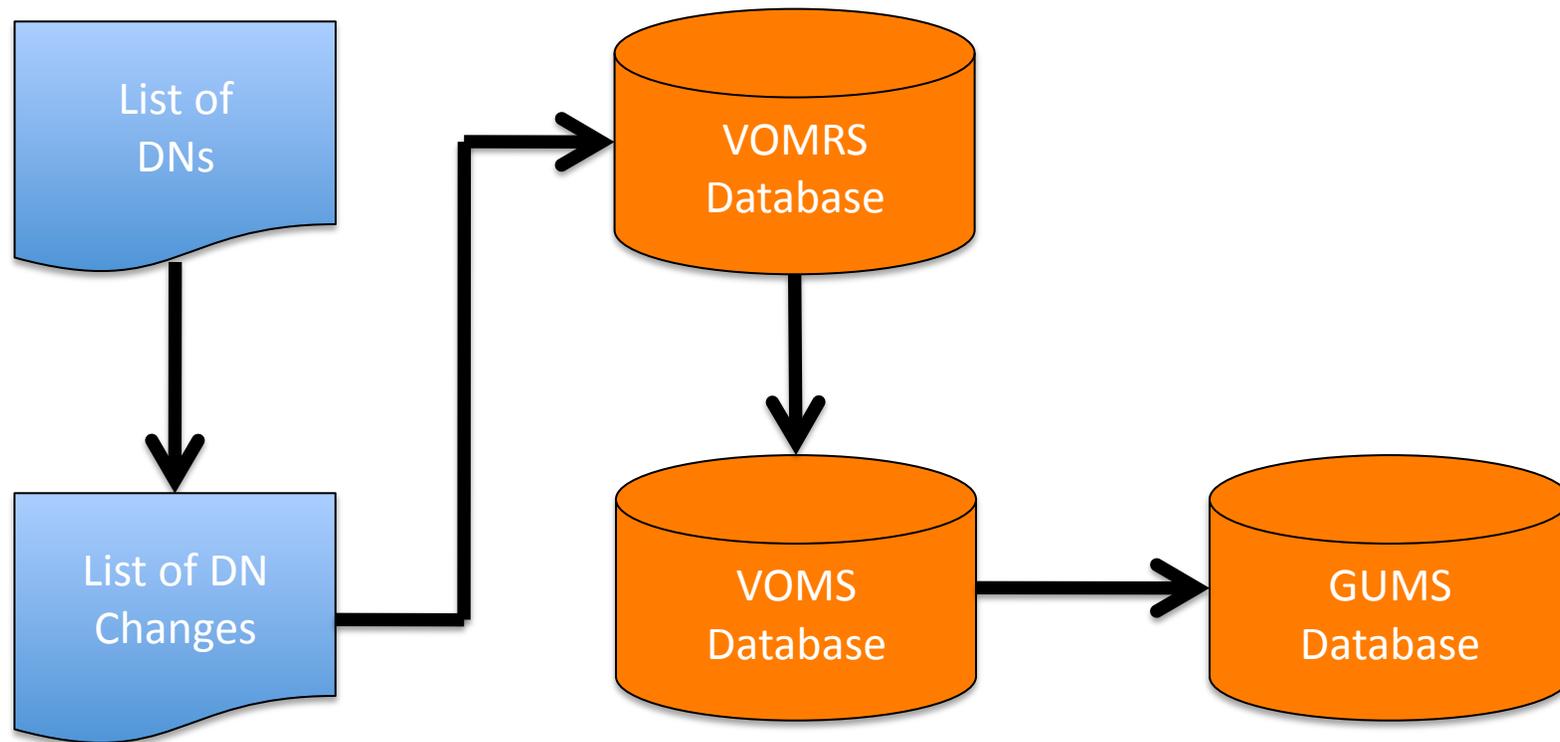
FermiGrid then automatically picks up the most recently published KCA DN list,

- Scans the list for any newly added DNs,
- Scans the list for any removed DNs.

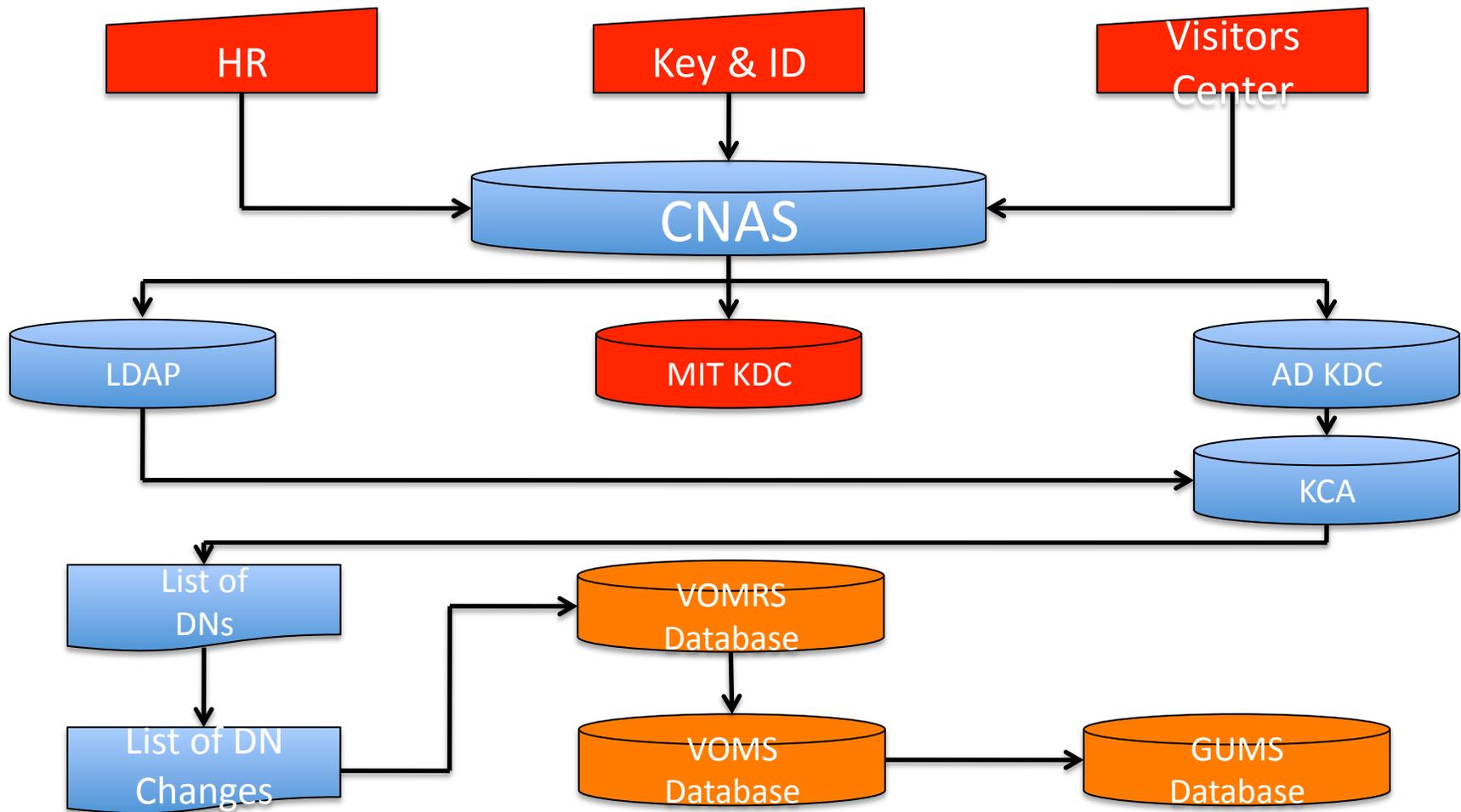
The corresponding changes are then propagated into the fermilab VO Grid authentication and authorization services:

- Virtual Organization Member Registration Service (VOMRS),
- Virtual Organization Management Service (VOMS),
- Grid User Mapping Service (GUMS).

Workflow - Diagram 3



Overall Registration Workflow



Deregistration

Departures are handled pretty much in the same way:

- On the last day of an employee, their CNAS record is marked as “inactive”.
- Others (contractors, visitors, etc.) have a limited CNAS lifetime, when the lifetime expires (and is not renewed), the corresponding CNAS record is marked as “inactive”.

The various scripts automatically pick up these changes and propagate them through the registration workflow.

Once an individual leaves Fermilab, their computer accounts and credentials (including Grid access) are typically terminated within one hour.

- There are out of band mechanisms to accomplish this faster if the situation warrants.

User Service Request Workflow

kinit

kx509 / kxlist -p

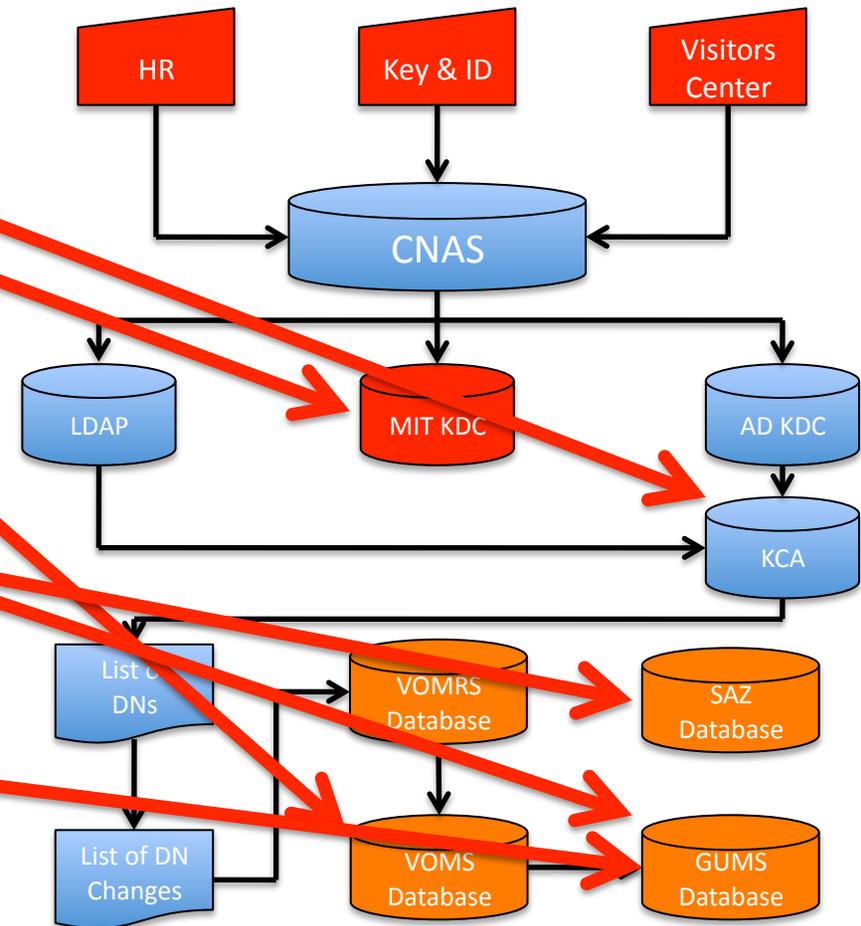
voms-proxy-init

globus-job-run

- globus-gatekeeper

globus-url-copy

- gridftp server



fermilab Virtual Organization?

What is the fermilab VO?

- It is an “umbrella” virtual organization for all people that have valid Fermilab Kerberos credentials,
- It is formally registered with the Open Science Grid.

Why have the fermilab VO?

- The VO management and operational infrastructure are optimized for large organizations such as CDF, DO, CMS and Atlas with >500 people that can afford to “pay” the necessary management and operational overheads.
- The experiments (groups) in the fermilab VO typically have an order of magnitude fewer people (25 to 50).
- The fermilab VO centralizes the management and operational FTEs and allows the smaller experiments to concentrate on doing the physics, rather than run services.
- The ability to create groups in the fermilab VO with lower overhead allows the fermilab VO to be more responsive to the physics / user community at Fermilab.
- Having the fermilab VO closely tied to the Fermilab Kerberos infrastructure allows the FermiGrid administrators to automate some of the VO administration and thus lower the operational “costs” to manage the VO.

The Fermilab KCA and the fermilab VO:

- The Fermilab Kerberos Certificate Authority is a key piece of infrastructure.
- An individual’s membership in the fermilab VO is directly tied to their (active) Kerberos credentials.

Kerberos Certificate Authority History

Event	Date
First Fermilab KDC Installed	~2001
Fermilab KCA Installed	Aug-2002
Fermilab KCA admitted to IGTF as an "experimental" CA	05-Jun-2004
Fermilab KCA configuration modified to replace the OIDs /UID=<name> and /USERID=<name> with /CN=UID:<name> in DN	28-May-2008
Redundant Fermilab HSM KCA Commissioned	11-Feb-2009
Redundant Fermilab HSM Based KCA accredited by IGTF	02-Jun-2009
Redundant Fermilab HSM KCA moved to Production & "experimental" Fermilab KCA retired	16-Nov-2009
"Experimental" Fermilab KCA removed from IGTF	10-Jun-2010

Why Change the KCA OID?

Various versions of openssl had inconsistent representations of the old OU=People OID:

- /DC=gov/DC=fnal/O=Fermilab/OU=People/CN=Keith Chadwick/UID=chadwick
- /DC=gov/DC=fnal/O=Fermilab/OU=People/CN=Keith Chadwick/USERID=chadwick

We tried various OIDs, that also wound up having inconsistent representations:

- /pseudonym=UID=chadwick /OID.2.5.4.65="UID=chadwick"
- /CN=UID=chadwick /CN=UID="chadwick"

The new OID that wound up working for all (tested) software was:

- /CN=UID:chadwick

KCA and Robots

One key feature of the Fermilab KCA is the ability to issue "Robot" credentials.

The "Robot" credentials are:

- Explicitly tied to the individual that requested the "Robot" credential be created,
- Explicitly tied to the "system" on which the "Robot" credential was generated,
- Explicitly tied to the mechanism that was/is used to generate the "Robot" credentials.

People and Robot DNs

OU=People:

- /DC=gov/DC=fnal/O=Fermilab/OU=People/CN=Keith Chadwick/
CN=UID:chadwick

OU=Robots (from kcron):

- /DC=gov/DC=fnal/O=Fermilab/OU=Robots/CN=fermigrid0.fnal.gov/
CN=cron/CN=Keith Chadwick/CN=UID:chadwick

OU=Robots (from CDF Glidein Factories):

- /DC=gov/DC=fnal/O=Fermilab/OU=Robots/CN=glidecaf/CN=cdf/
CN=Keith Chadwick/CN=UID:chadwick
- /DC=gov/DC=fnal/O=Fermilab/OU=Robots/CN=namcaf/CN=cdf/
CN=Keith Chadwick/CN=UID:chadwick

KCA - Interactive vs. Kcron

Interactive	Kcron
login to system	kcroninit (once)
----	----
kinit	kcron <script>
----	----
kx509	kx509
kxlist -p	kxlist -p
voms-proxy-init	voms-proxy-init
globus-job-run	globus-job-run
globus-url-copy	globus-url-copy

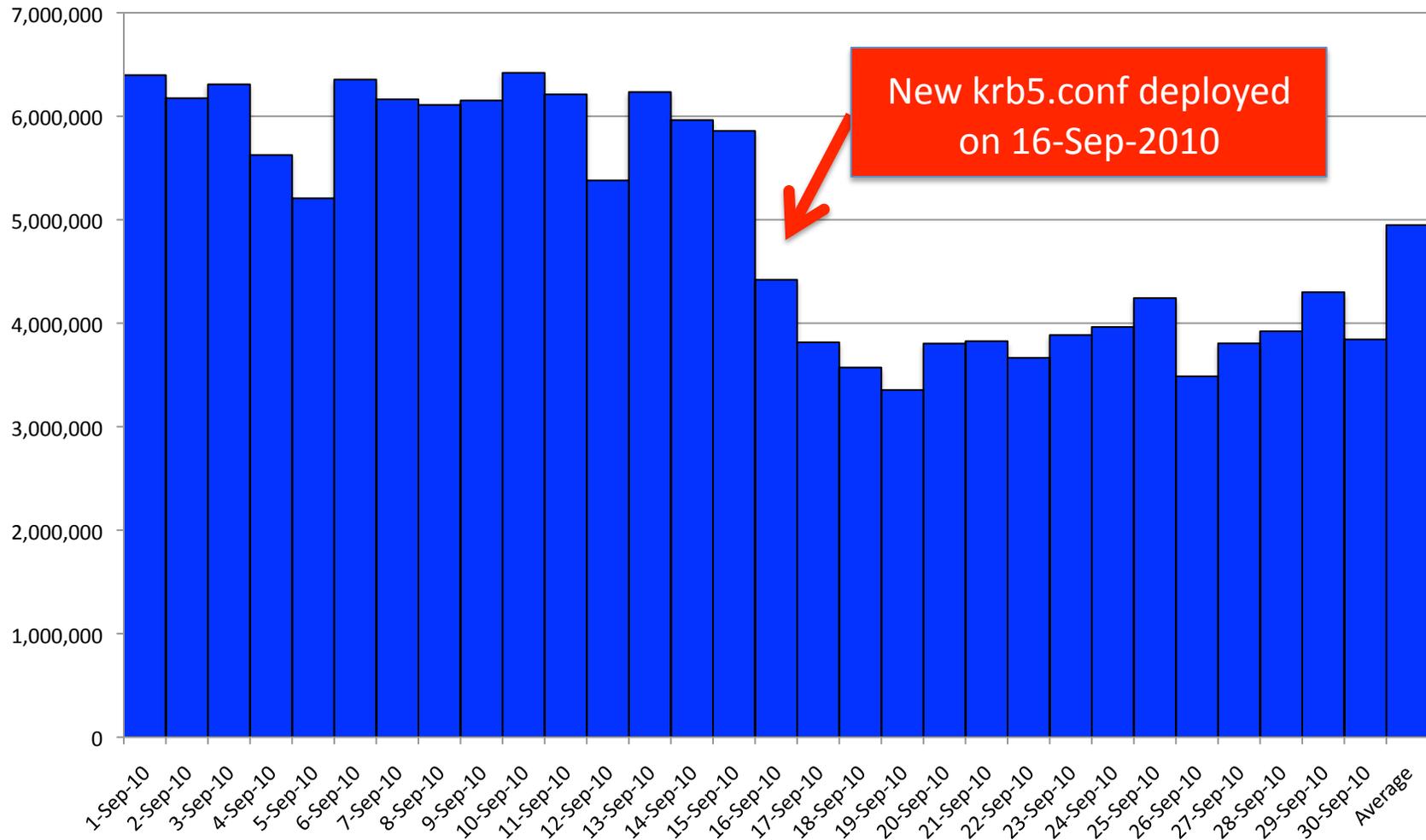
Fermilab KCA vs. D0Egrids

Fermilab KCA	D0Egrids CA
<p>OU=People:</p> <ul style="list-style-type: none"> • Default Lifetime 26h • Maximum Lifetime 7d • Renewable No • Password No 	<p>OU=People:</p> <ul style="list-style-type: none"> • Default Lifetime 1y • Maximum Lifetime 1y • Renewable Yes • Password Yes
<p>OU=Robots:</p> <ul style="list-style-type: none"> • Default Lifetime 12h • Maximum Lifetime 3d • Renewable No • Password No 	<p>OU=Services:</p> <ul style="list-style-type: none"> • Default Lifetime 1y • Maximum Lifetime 1y • Renewable No • Password No

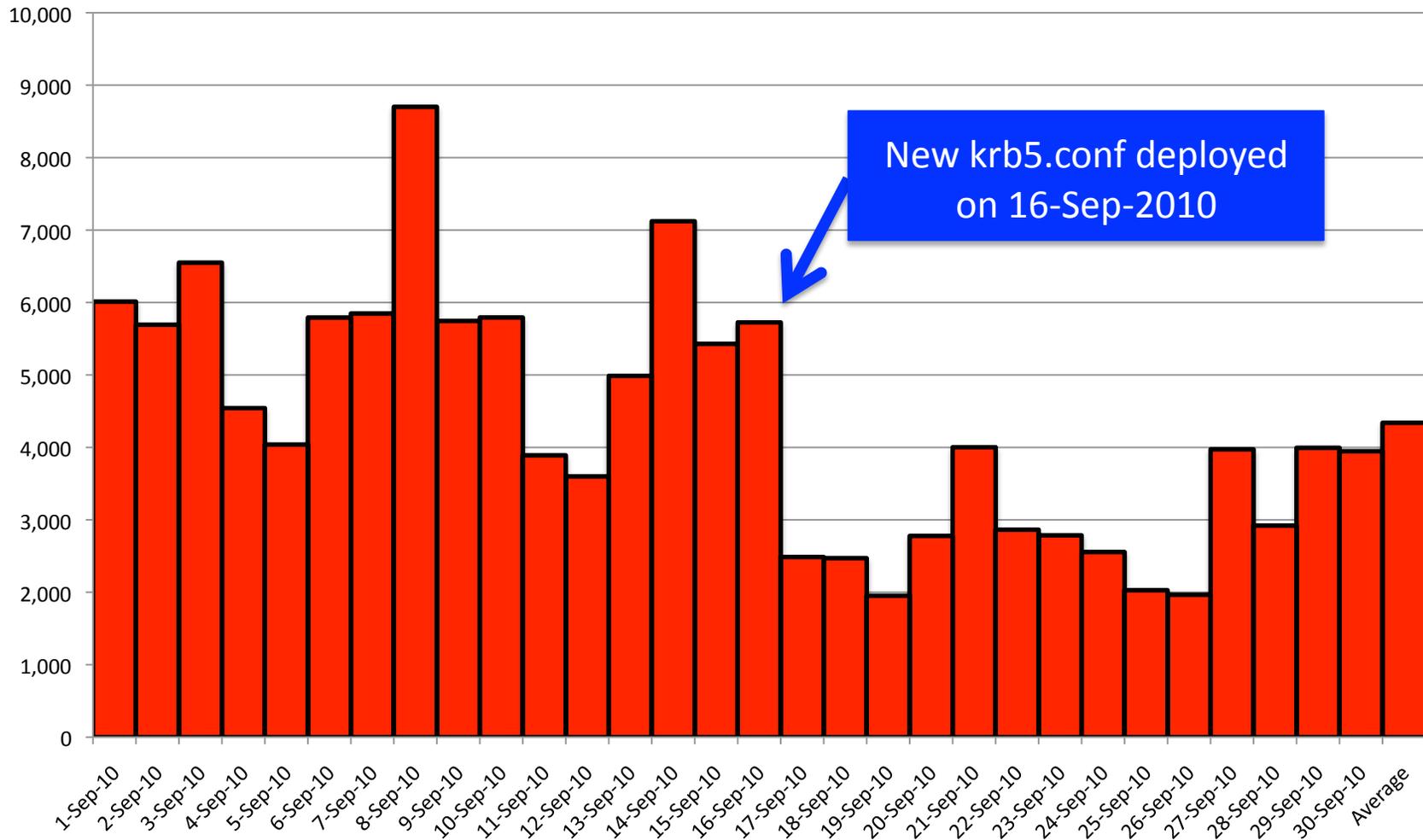
Some Statistics

Statistic	Value
# of MIT KDCs	8
# of AD KDCs	5
# of HSM KCAs	2
# of Fermilab OU=People DNs	5168
# of Fermilab OU=People DNs that have been used to run a Grid job	125 (2.4%)
# of Fermilab OU=Robots DNs	9374
# of Fermilab OU=People DNs with at least one Robot	1911 (37%)
# of Fermilab OU=Robots DNs that have been used to run at least one Grid job	753 (39%)
Average # of MIT Kerberos tickets/day	~5,000,000
Average # of KCA certificates/day	~4,350
# of fermilab VO voms-proxy-init requests/day	645 Avg 1,700 Max
# of cdf VO voms-proxy-init requests/day	507 Avg 4,100 Max

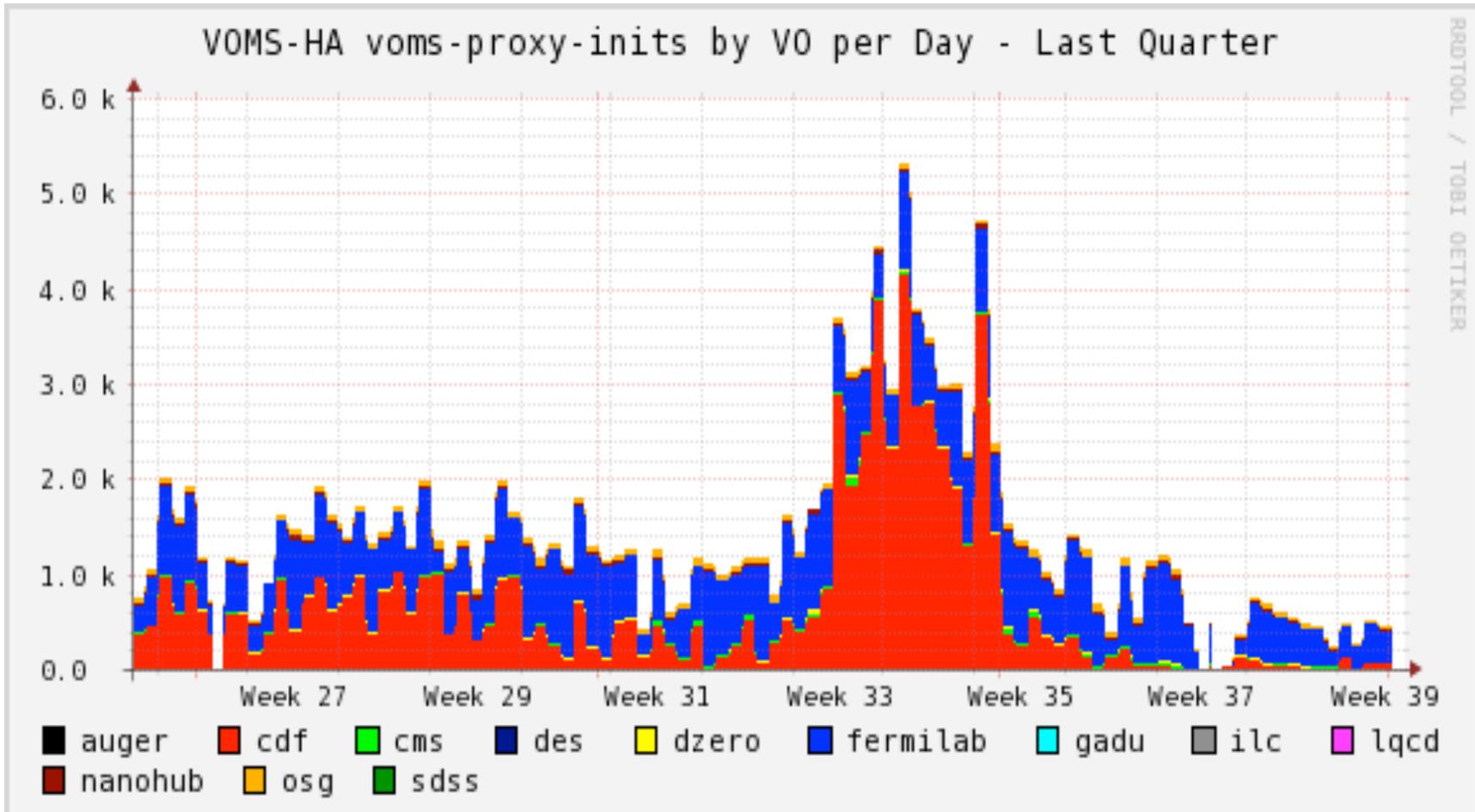
Kerberos Tickets / Day



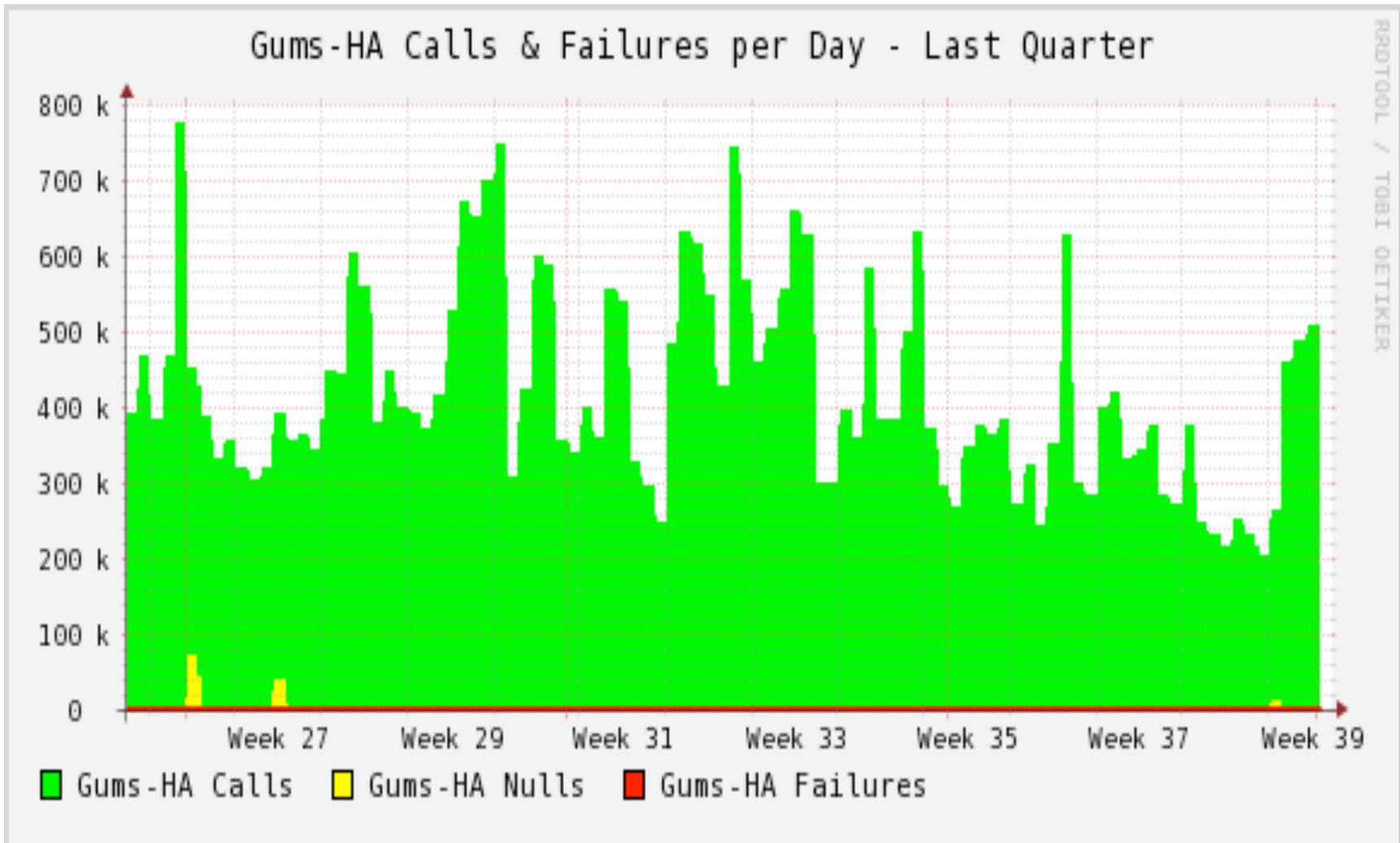
KCA Certificates / Day



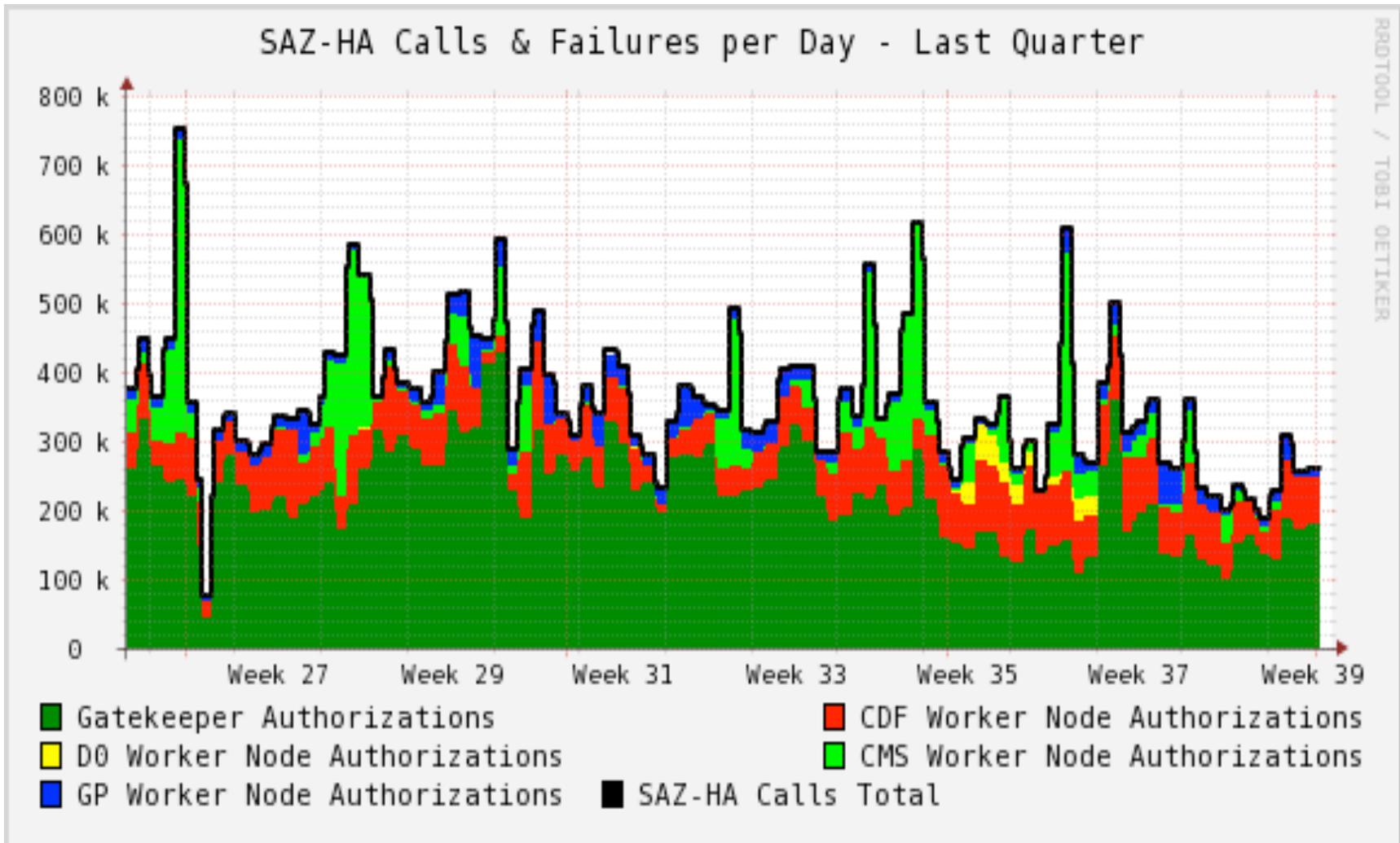
voms-proxy-inits / Day



Gums Mappings / Day



SAZ Authorizations / Day



Services Authentication at Fermilab

“Services” accounts can be used for authentication to various services:

- Service Desk
- VPN
- Email
- Electronic Time Cards
- Etc.

In the event that an individual loses or forgets their “services” account password, they can reset it using their “Strong” authentication account.

Future

Fermilab has just started the project to migrate from the home grown CNAS system to an identity management system based on Oracle Identity Management Services (OID).

The replacement for CNAS will be known as Fermi Single Source of Truth (FSST).

We are also investigating InCommon and Shibboleth.

Summary

Fermilab is both an identity provider and a relying party of other identity providers.

The Fermilab Kerberos Certificate Authority is a key piece of infrastructure.

The “services” domain has allowed Fermilab to deploy commercial (“industry standard”) software with a lower effort profile that would have been required to recode and maintain the applications in-house.

We are actively working on moving other components of the Fermilab identity management stack from in-house written code to commercially written and supported software.

Fin

Any Questions?