A Middleware Unified Field Theory

Identity Management / Directories

Privileges / Groups

Single Sign-On / Federation

Diagnostics?

Enterprise Integration

from network to application

Michael R Gettes
MIT
11-2007 & 10-2009

An interpretation of the original MACE mission

What do we want?

Inter-Enterprise Workgroup COllaborations

not sexy

or

Collaborative

Organizations

co

Identity

Groups

Privileges

Federated Access

and …

Applications

"It's all about the App stupid!"

Give

COntrol

To

COmmunity Members

Integrate with Existing COmmon IT Infrastructures

in

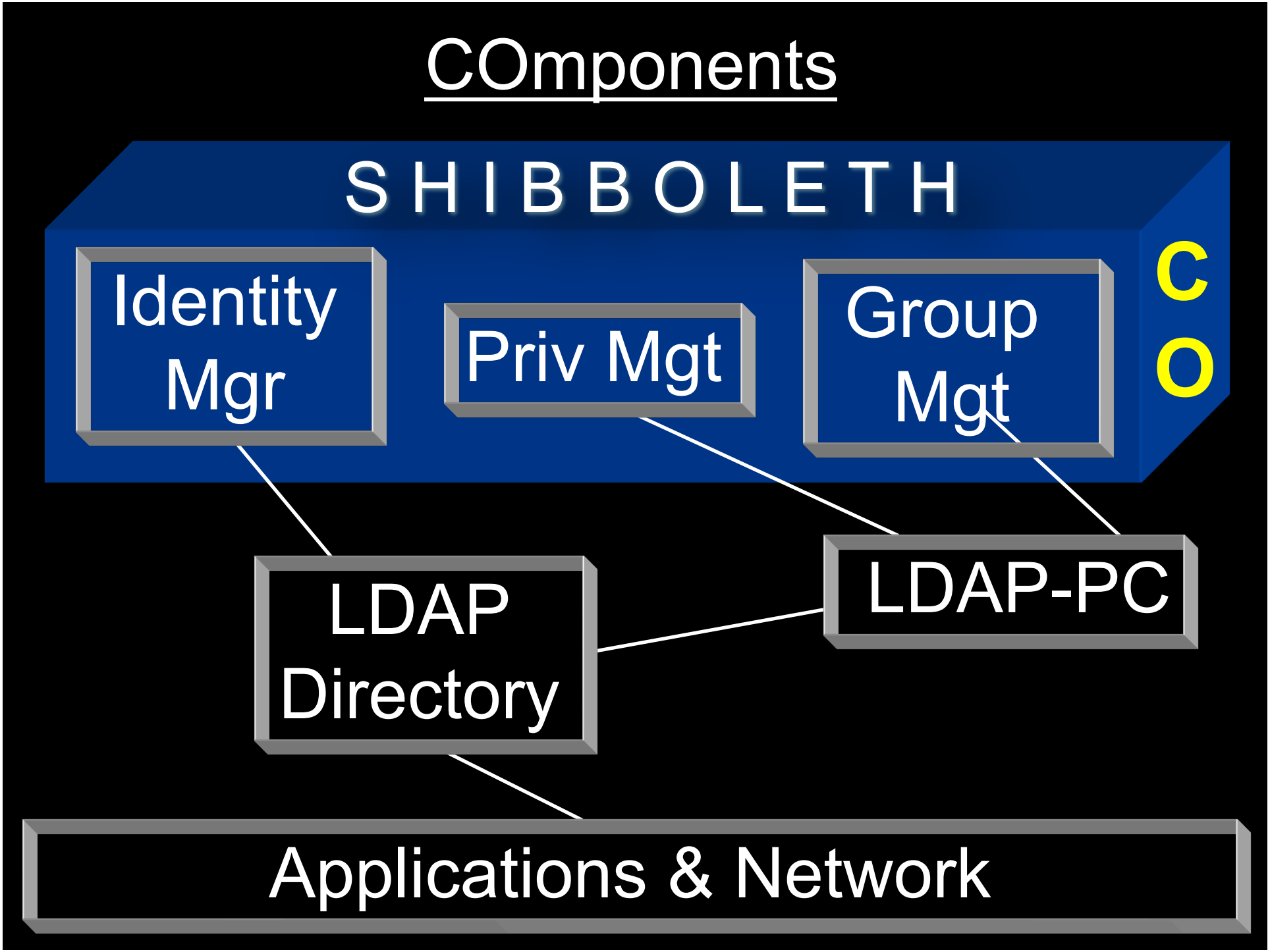
Higher Education

Flexible

Scalable

Modular

InCommon™

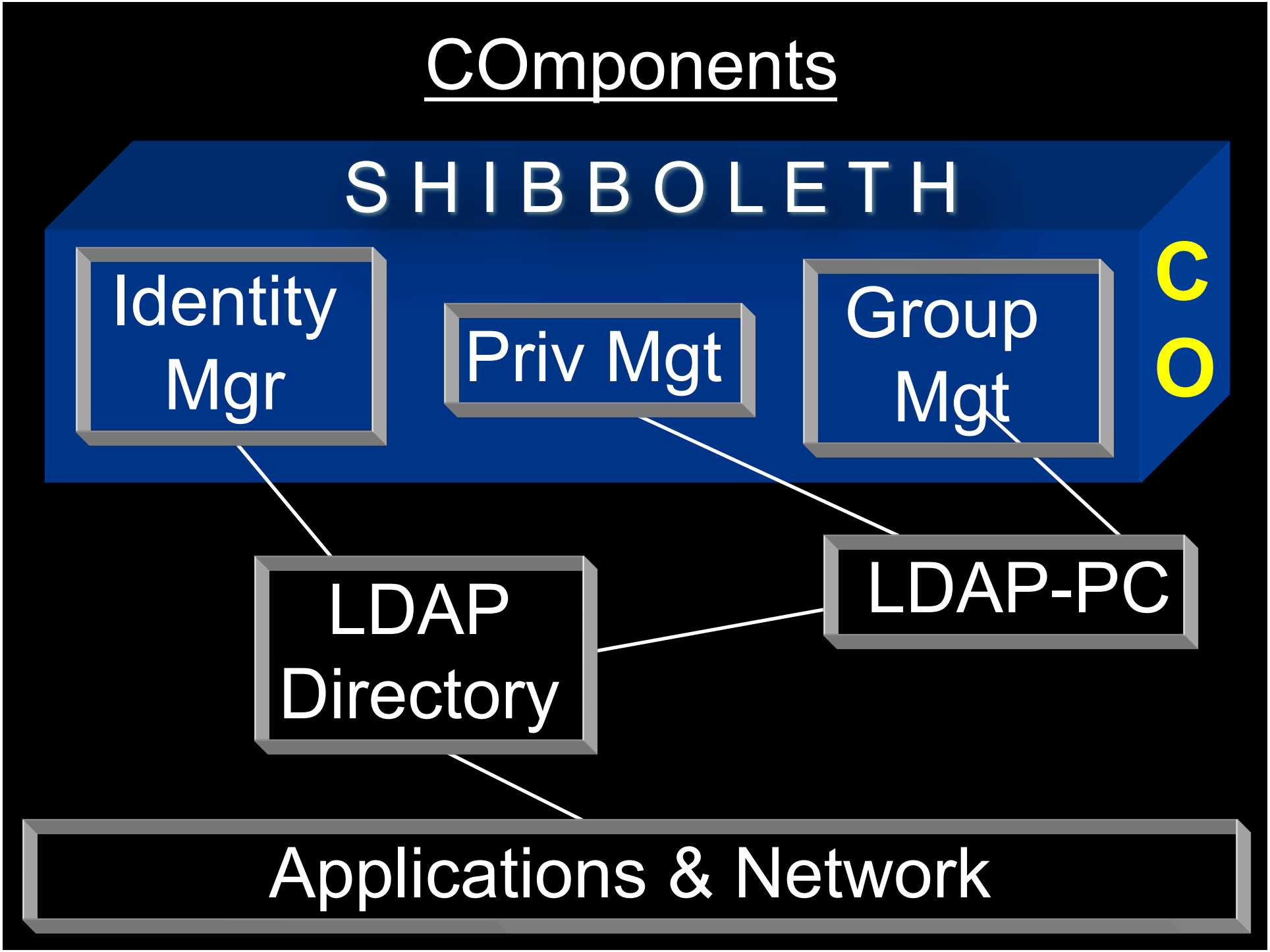

COmponents
S H I B B O L E T H
Identity Mgr
Priv Mgt
Group Mgt
C O
LDAP Directory
LDAP-PC
Applications & Network

stop talking

start walking

demo

CO.internet2.edu


COmponents
S H I B B O L E T H
Identity Mgr
Priv Mgt
Group Mgt
C O
LDAP Directory
LDAP-PC
Applications & Network

COmanage …

is a demonstration of
the CO model

a CO fits within a service delivery strategy

Stuff stored in Directories

(everybody has one)

Directories make Priv/Group data more accessible

Application Management

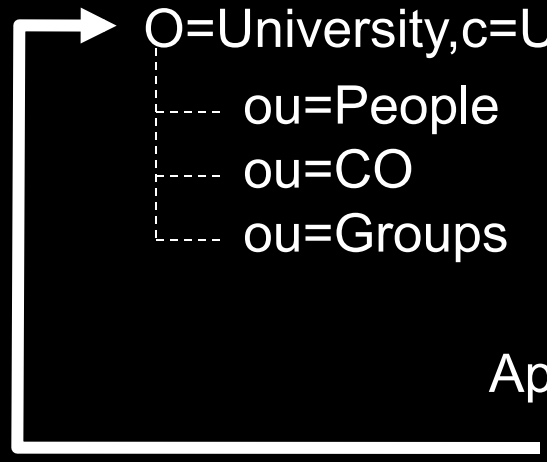
App Access to data is managed by LDAP (initially)

Identity data can be distributed by any desired mechanism in the future. SQL databases, feeds, message bus technologies.

No local identity issued for external users to access CO services

big win!

Example directory tree for CO environment



(this is where 50K fac/staff/stu might reside)
(external identities for CO go here)
(a place to store groups for all)

Applications pointed here for identities
yields the union of internal and external

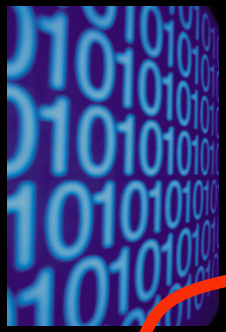
Future…

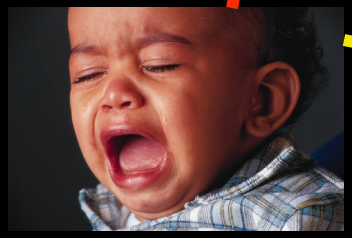
Begin addressing issues of “attribute eCOnomy”

Protect CO by Identity Provider…

can solve “IEEE problem”?

Web site wants to know: Are you a member of IEEE?



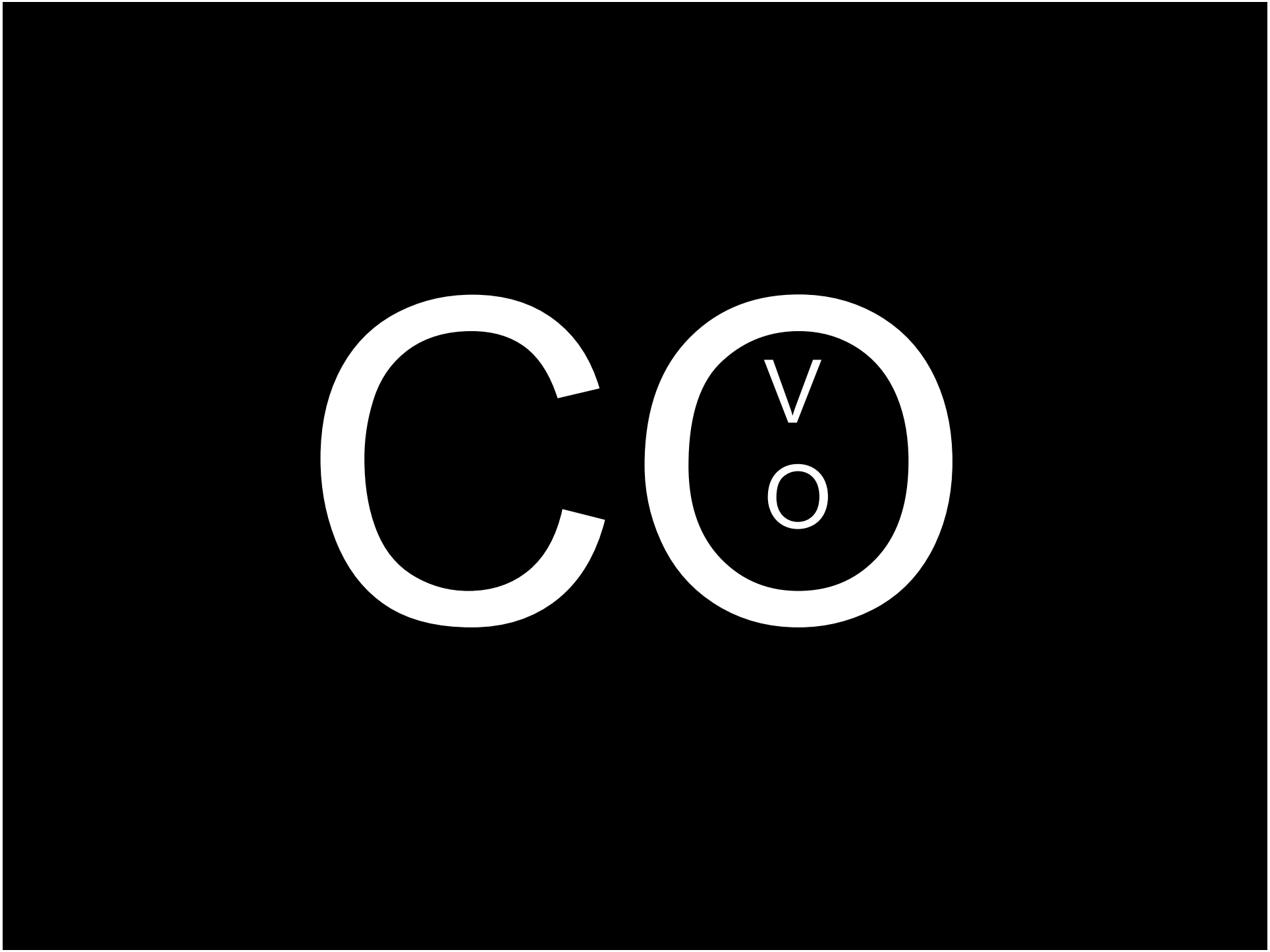


User

My University

Home Identity Provider

IEEE-CO
This org has membership data but does not manage identity - a CO with only external users.

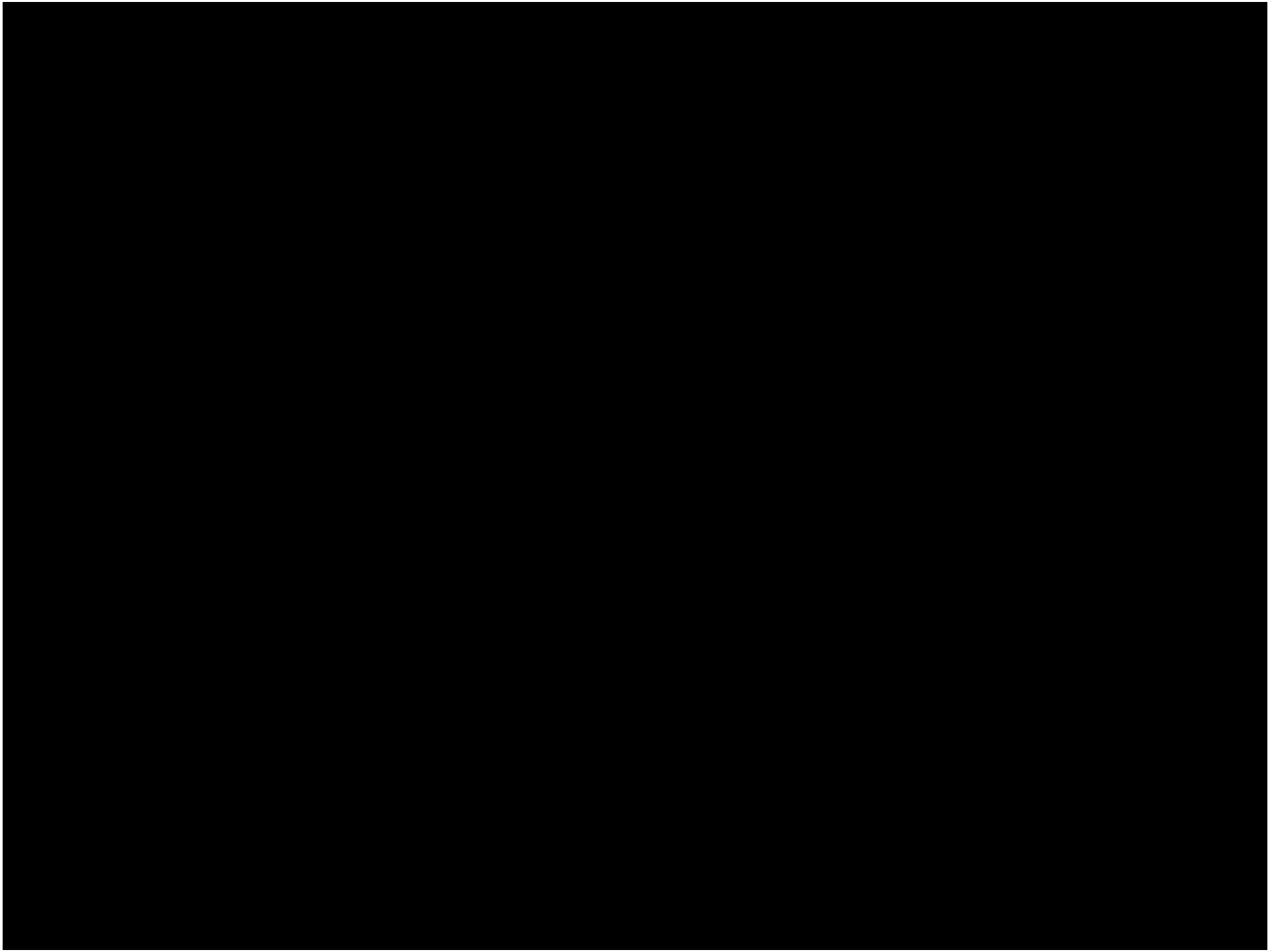

CO
V
O

a service of InCOmmon?

done

http://middleware.internet2.edu/co

Talk amongst yourselves



Diagnostics

Lifting up shib log files
and making EDDY deposits

Creating a unified and federated view of diag data

- Network data: flows, snort, snmp
- System stats: cpu, i/o, mem, etc…
- Infrastructure: shib, ldap, authN, etc…
- Application: http, confluence, sympa, calendar

etc, etc, etc…

http://web.cmu.edu/eddy

http://www.fudgie.org

Network Layer?

Why not?

Integrate with Grids?

Why not?

Addresses VO scenarios?

Why not?