

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

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

SHIBBOLETH

Identity
Mgr

Priv Mgt

Group
Mgt

C
O

LDAP
Directory

LDAP-PC

Applications & Network

stop talking

start walking

demo

CO.internet2.edu

COmponents

SHIBBOLETH

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

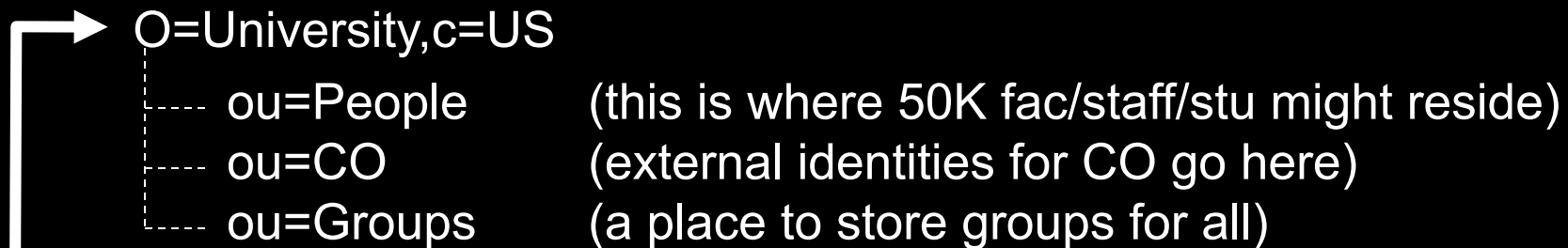
App Access to data is
managed by LDAP (initially)

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



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

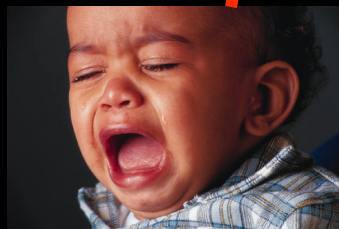
Future...

Begin addressing issues of “attribute eCOonomy”

Protect CO by Identity Provider...

can solve “IEEE problem”?

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



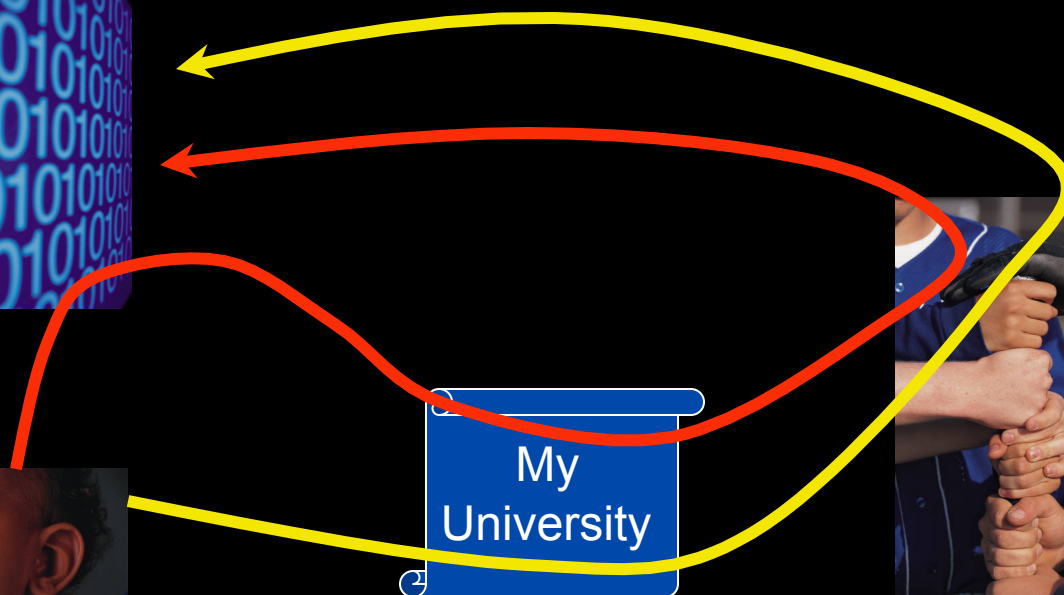
User



Home Identity Provider



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



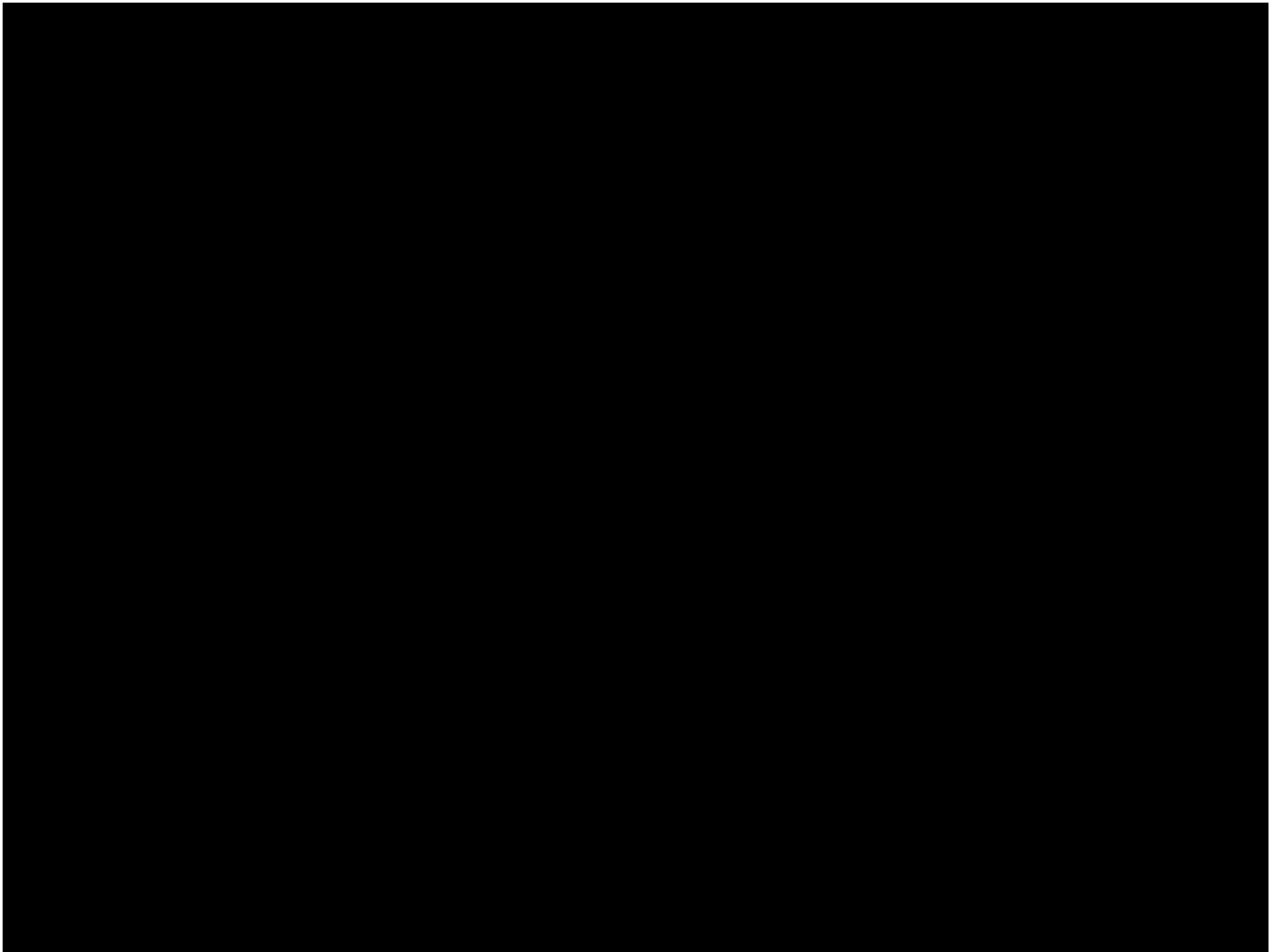
COVO

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, sympy, calendar
etc, etc, etc...

<http://web.cmu.edu/eddy>

http://www.fudgie.org

INFO		URLS	
Logins	33	35.75	/nl/actionhandler.pl
SITES		32.24	/action.pl
managerleague.com	432.35	30.36	/nl/general.pl
fudgie.org	56.51	26.22	/nl/playerinfo.pl
mrsfudge	32.24	23.01	/nl/team.pl
dge.clockingit.com	8.33	22.50	/nl/teaminfo.pl
www.clockingit.com	0.83	22.98	/nl/pages/main.php/muhe
kai.clockingit.com	0.75	18.47	/nl/preferences.pl
856.ct88r8ttt:888	0.65	15.25	/
oee.clockingit.com	0.55	13.22	/nl/offers.pl
ude.clockingit.com	0.48	11.60	/managerleague.pl
CONTENT		10.95	/game_login.pl
page	465.25	9.61	/nl/messages.pl
image	50.63	9.00	/nl/transfer.pl
javascript	1.97	8.71	/tasks/update_sheet_inf
css	1.93	SLOW REQUESTS	
flash	0.69	1.48	/timeline/list
movie	0.60	0.71	/activities/list
STATUS		0.19	/feeds/ical/bb9a15580ea
200	452.21	0.19	/feeds/rss/09208886888d
304	54.45	0.14	/forums/index
302	13.42	REFERRERS	
301	1.02	73.05	-
USERS		1.74	https://www.kakleriet.no
85.196.112.106	53.97	0.87	http://www.google.it/se
86.147.213.126	17.06	0.80	https://www.kakleriet.no
85.164.221.90	8.84	0.65	http://www.kakleriet.no
84.202.62.25	8.46	0.43	http://209.85.135.104/s
89.129.17.26	8.23	0.30	http://www.google.no/se
85.167.49.50	8.33	0.14	https://www.google.es/se
86.90.98.56	7.35	USER AGENTS	
80.202.163.24	6.15	46.18	Mozilla/4.0 (compatible
80.202.101.133	5.21	31.56	Mozilla/4.0 (compatible
88.197.162.58	4.18	31.02	Mozilla/4.0 (compatible
		30.35	Mozilla/4.0 (compatible

Network Layer?

Why not?

Integrate with Grids?

Why not?

Addresses VO scenarios?

Why not?