

Identity Management Systems for Collaborations and Virtual Organizations

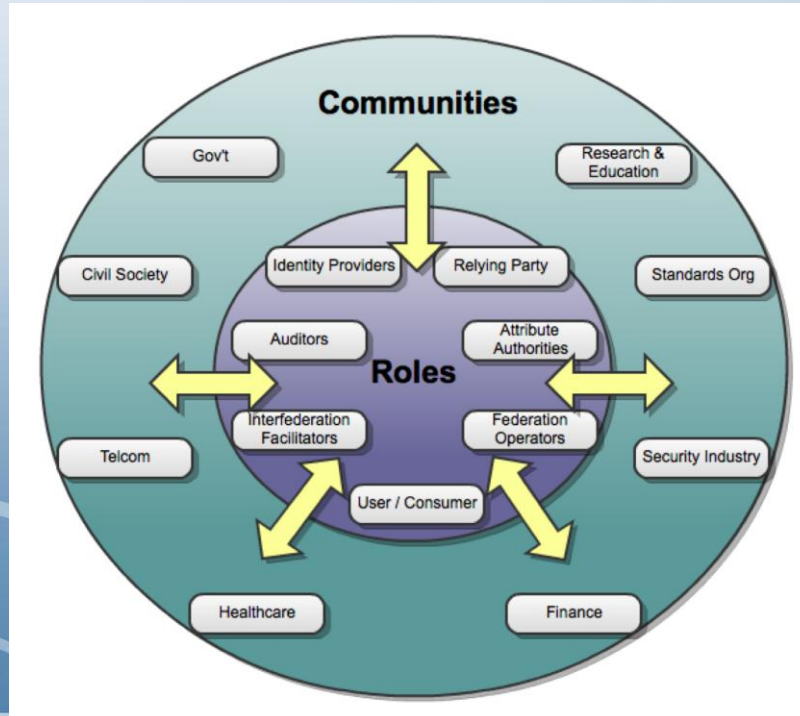
Topics

- Update on Internet identity
- IdM Systems for Virtual Organizations
 - Goals
 - Early Implementations
- Issues and Discussions

Update on Internet identity

- Consumer marketplace update
 - OIX players, Facebook, OpenId Connect, Monetized Attribute Authorities
 - National Strategy for Trusted Identities in Cyberspace
- Federated identity update
 - InCommon and international federations
 - Non web apps – OAuth, Moonshot and Kitten
 - Social2SAML and other bridges
- InCommon update, including certs, silver, NSF, uApprove
- Mapping the Identity Ecosystem – ISOC activities

Identity Ecosystem Players, ISOC view



Consumer marketplace update

- Several major “identity providers” (Google, Paypal, Yahoo) attempting to converge on a new standard, OpenId Connect.
 - OIX (Open Identity Exchange) is the hub
 - Technically Shibboleth++ redone in JSON
 - Uses SAML attributes and SAML metadata, allowing integration
 - Differs on discovery, marketplace vision, government
 - Some are coupling with mobile operators for higher LOA
- Others sitting on sidelines – Facebook, Twitter

The roles and attributes of consumers

It is important to differentiate the roles, and associated attributes of individuals (distinct from roles/attributes from their work)

- Consumer
- Citizen
- Enterprise/vertical
- Geo-temporal
- Personal “wallet”

Same identity; different roles; different policies and governance

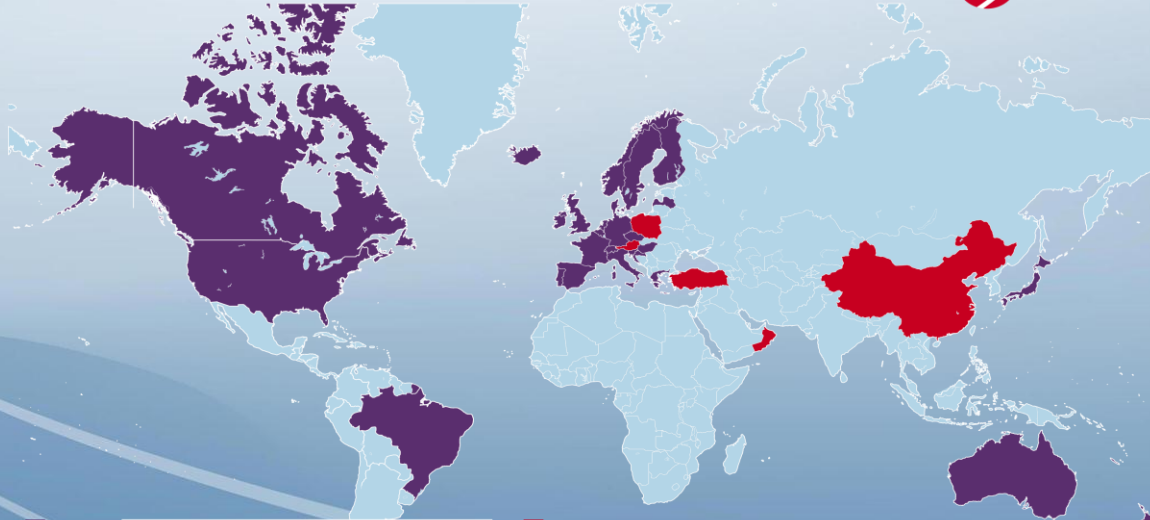
How transparent to make the change of roles

NSTIC Update

- NSTIC - <http://nist.gov/nstic/>
 - Well-crafted architecture and approach
 - Faces challenges with limited resources, mixed motives for IdP's, other federal players, etc
- OMB Directive issued Fall of 2011 to move to external identities where appropriate
- IDTrust Conference March 13-14, 2012

R&E federations

Research and Education Identity Federations



Identity Federations in production

AU	Australian Access Federation AAF	IE	Edugate
BE	Belnet R&E Federation	IT	IDEM
BR	CAFe	JP	GakuNin
CA	Canadian Access Federation CAF	LV	LAIFE
CH	SWITCH.ch	NL	SURFfederatie
CZ	eduD.cz	NO	FEIDE
DE	DFN-AAI	NZ	Tuakiri New Zealand Access Federation
DK	WAYF	PT	RCTSaai
ES	SIR	SE	SWAMID
FI	Haka	SI	Arnes-AAI Slovenska
FR	Fédération Education-Recherche	UK	UK Access Management Federation for Education and Research
GR	GRNET	US	InCommon
HR	AAlasEduHr	int	IGTF
HU	eduD.hu		

Identity Federations in pilot

AT	ACOnet-AAI Federation
CN	CARS
OM	OMAN_AID
PL	Poland Identity Federation
TR	ULAKAAL

This map is intended to provide a high-level overview of countries with identity federations.

Last update: 15 April 2011

InCommon today



- 250+ universities, 450+ total participants, growth still rapid
- > 10 M users
- Traditional uses continue to grow:
 - Outsourced services, government applications, access to software, access to licensed content, etc.
- New uses bloom:
 - Access to wikis, shared services, cloud services, calendaring, command line apps, UHC, Mayo, etc.
- Certificate services bind the InCommon trust policies to new applications, including signing, encryption, etc.
- Officially FICAM certified at LOA 1 and 2 (Bronze and Silver).

Important New Services

- Research.gov
 - Includes NSF Fastlane
- Electronic grants administration from NIH
- Growing use in Esnet
- CILogon (cilogon.org)
- Mayo Clinic, UHC, National Student Clearinghouse
- IEEE, Educause
- NBCLearn, Desire2Learn, PeopleAdmin, Qualtrics
- UniversityTickets, Students Only Inc, StudentVoice

InCommon – a work in progress

- Growth and managing growth
- Silver – higher levels of assurance
- uApprove – end user attribute management
- Solidifying member participation
- Social2SAML coordination
- Personal certificates
 - Powerful old technology for authentication, signed email, signed documents, encryption, etc.
 - Soon to be a major user of federated identity

Silver

- Higher assurance profile to deal with access of a financial or valued resource
 - Electronic grants administration, Teragrid, OSG, medical records, etc.
- A careful walk between what's feasible on campuses and what agencies would like
- Includes some type of audit by InCommon (possibly review of exceptions to common practice)
- Fresh baked, unpriced yet
- <http://www.incommon.org/assurance/>

When to do Consent

- Not at all – part of an existing contractual relationship
- At the point of collection of information
 - “We intend to use what you give us in the following ways”
- At the point of release of information
 - “I authorize the release of this data in order to get my rubber squeeze toy...”
 - Per transaction or persistent for some time

R&E basic attributes (eduPerson et al)

- High-level affiliation (eg, member, faculty, staff, student)
- Opaque, persistent and non-correlating identifiers (ePTID)
- A persistent and human-usable identifier (eg, kjk@internet2.edu)
- Name (e.g. Display Name)
- Email address
- An open-ended set of entitlements assigned by the institution, including group membership

Bundles and Application Categories

- Attributes tend to travel in bundles
 - The R&S (research and scholarship) bundle
 - {name, email, authenticated identity, affiliation}
 - Applications are being vetted for minimal use and qualification for R&S
 - Attribute release automatic
- Several bundles are likely, e.g. {opaque-id, affiliation}, {authentication only}

Non-web apps

- A variety of approaches are being developed to address these large families of apps
 - Challenges are discovery, trust anchors in the clients, attribute release and privacy management
- Three categories of approaches
 - Moonshot - GSS over Radius (and maybe SAML)
 - Oauth and OpenId-Connect
 - SAML ECP (extended client profile) - Kitten
- Lots of hope but no turn-key deployments yet

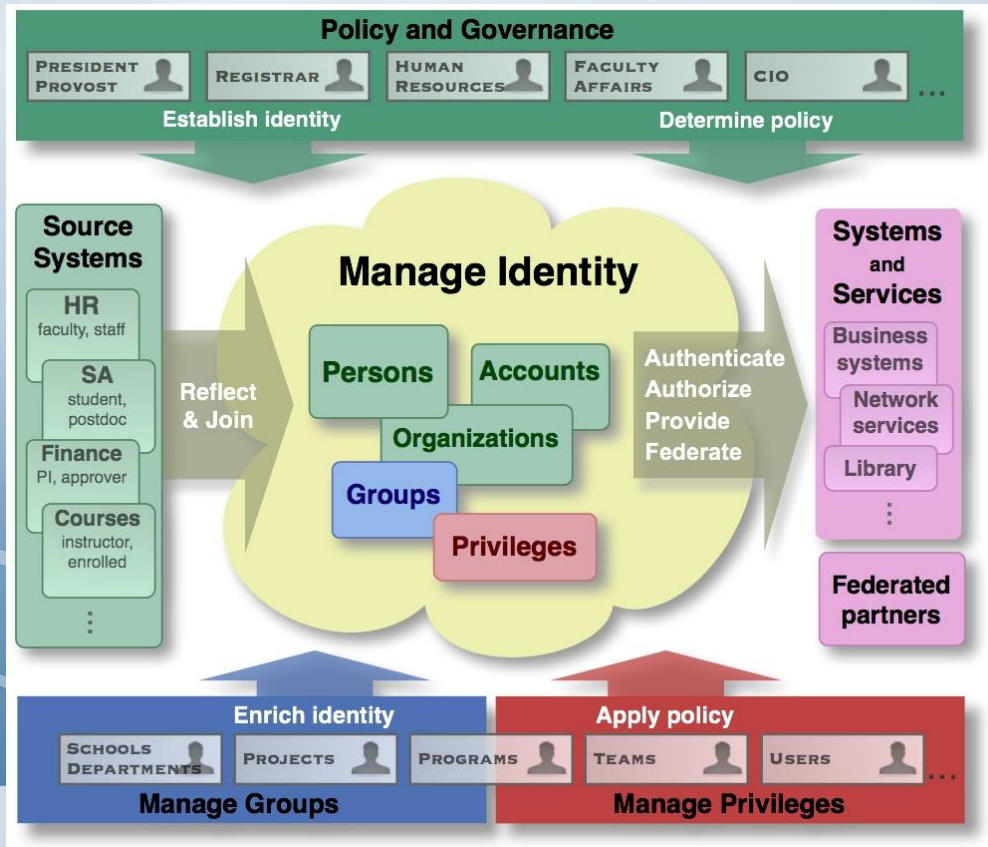
Interfederation

- Connecting autonomous identity federations
- Critical for global scaling, accommodating state and local federations, integration across vertical sectors
- Several operational “instances” – Kalmar2 Union, eduGAIN
- Has technical, financial and policy dimensions
- Key technologies moving forward – PEER, metadata enhancements and tools, discovery

Context for VO Identity Management

- Three contexts to think in
 - Internet-scale
 - Campus/Enterprise
 - Virtual Organization (VO)
- The key issue in the discussion is how to leverage Internet and enterprise to serve the VO
 - Leverage for security, privacy, efficiency, ease of use, sustainability, etc.
 - Identify and engineer that which is unique to the VO

Campus Identity Management



VO Identity Management

- Control the access to VO resources to properly authenticated and authorized users
- Serve deep (high-security bio research with complex and diverse data access needs) and wide (outreach to large educational communities) and international
- Identity Management applied to non web applications, to devices, to processes, etc
- Integrate with scholarly identity
- Limited support resources, internal competition, legacy apps, ad hoc authority and processes

ABC: A Typical Use Case of VO IdM

- Has 50 researchers who can schedule ABC instruments, run compute jobs on the TG with ABC allotments, etc
- Has 500 academics who need access controlled wikis, ad hoc calendaring (ala Doodle), lists, VO event calendaring, file sharing, chat rooms, videoconferencing, etc.
- Has administrators at fifteen universities who can access rosters, change roles, etc.
- Has partner VO's in other countries, with varying privileges on what they can see and use on ABC resources
- Has outreach coordinators at 50 school districts who can post/read to certain wiki sections
- Works closely with publishers, funding agencies, etc.

Goals

- Leverage existing IdM technologies
- Leverage existing IdM deployed infrastructure
- Drive identity and access control for both general collaboration and domain-specific apps
- Connect to the scholarly record
- Offer a variety of implementation and deployment options
- <https://spaces.internet2.edu/display/COmanage/Video>

Collaboration Management Platforms

- An integrated “collaboration identity management system”
 - Provides basic group and role management for a group of federated users
 - Plugs into federated infrastructure to permit automatic data management
- A growing set of applications that derive their authentication and authorization needs from such external systems
 - Collaboration apps – wikis, lists, calendaring, netmeeting
 - Domain apps – instruments, databases, computers, storage
 - <https://wiki.surfnetlabs.nl/display/domestication/Overview>

CMP

- Next generation portal/gateways
- Intended for federated users and multi-domain applications
 - plumbed into the infrastructure
- More secure, more powerful, more privacy preserving, more application possibilities, more...

From the collaboration perspective

Scalable actions expected (or at least hoped for) in a CMP:

- Create and delete/archive users, accounts, keys
- Group management on an individual and CMP-wide scale
- Permit or deny access control to wiki pages, calendars, computing resources, version control systems, domain apps, etc.
- Manage cloud based collaboration services such as Adobe Connect and Cisco Webex
- Domesticated applications to meet the needs of the VO
- Usage reporting
- Metering and throttling
- All working across borders, constituencies, etc.

CMP under the hood

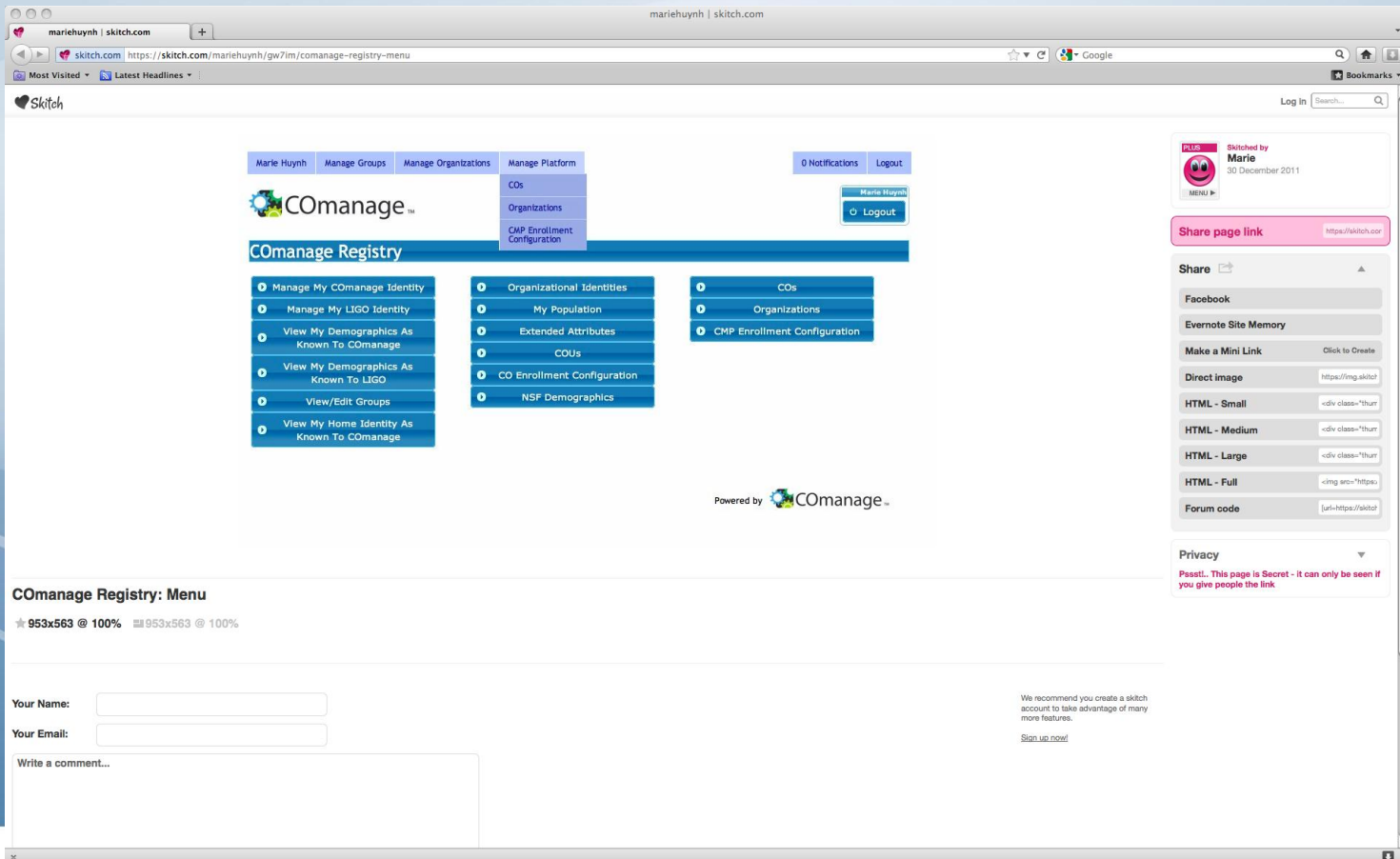
- A combination of enterprise tools refactored for VO's
 - Shib, Grouper, Directories, etc
- A person registry with automated life-cycle maintenance
 - Includes provisioning and deprovisioning
- A place to create, maintain local attributes
 - Using Groups and Roles
- A place to combine local and institutional attributes for access to applications
- A place to push/pull attributes to domesticated applications
 - Collaboration apps – wikis, lists, net meetings, calendars, etc
 - Domain apps – SSH, Clusters, Grids, iRods, etc.
 - Attributes delivered via SAML, LDAP, X.509, etc

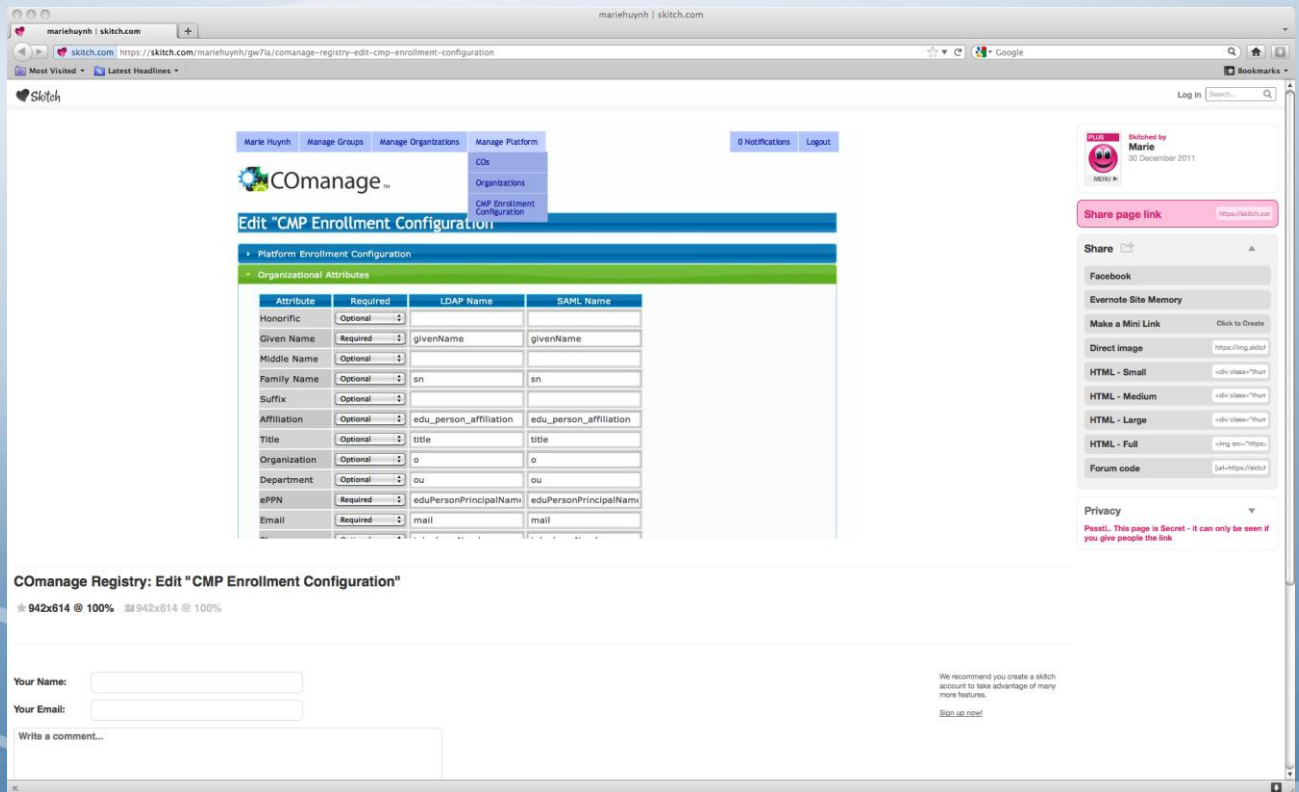
Examples of CMP's, or parts thereof...

- Surfnet
 - A thin national collaboration service, with no hosted applications, providing federation, groups, provisioning API's
 - A research collaboration service, with both hosted collaboration and integrated domain applications
 - All driven by SurfConnex, an open-source CMP that integrates Shib, Grouper, OpenSocial interfaces, etc.
- CManage
 - Tools and parts to integrate a CMP service into portals and gateways – LIGO and iPlant

Other examples

- National R&E efforts in Norway, Switzerland, Japan, and elsewhere
- Projects like GlobusOnline have overlapping elements
- Others?





Issues for MAGIC participants

- How does this vision mesh with the various agency views?
- How can VO's be informed of these tools?
- What are possible higher level CI deployment options for agencies?