Jasig Sakai 2012-06-11

CIFER (Community Identity Framework for Education & Research):
Open Source Identity Management for Higher Education (neé OSIdM4HE)

Ben Oshrin, Oshrinium LLC & Keith Hazelton

triggered by Oracle's purchase of Sun and deprecation of Sun Identity Manager

Elements of solution in open source: CAS, Shibb, Grouper, OpenAM, OpenIDM, 389, OpenLDAP, OpenDJ

Commercial: Pieces but little integration & missing aspects: multiple affiliations, distributed admin, multilateral federation, level of assurance

Open Source: good for R&E but missing: identity registry, provisioning, end user UIs

Home grown: tailored, but most expensive (if you count time of staff) and risky

CIFER Objectives:

Provide complete suite
competitive and complementary to big commercial IAM suites
Build on existing R&E IAMI software: Grouper, Kuali Identity Management, Shibb, CAS, Kerberos

Want to leverage existing things, be able to integrate with existing partial commercial or open source deployments

Add integration and process automation for reduced ops costs via improved delegatio, monitoring, reporting, compliance, and audit

Focus on challenges distinctive to HE

Avoid vendor lock

Work plan:

5 workstreams: registries, provisioning & integration, access management, authN, process automation

2 year build, then self-sustaining

Organization:

relation to I2, Kuali, Jasig; but not solely within any of those

AuthN workstream: non-web authN, account management tools, certs, 2 factor, mobile authN, social identities

Provisioning & Integration workstream: provisioning = outbound from registry; integration more general;
leverage existing tools such as Apache ServiceMix or other ESBs

Registries: ID Match (Open EMOI? or MDM tools?), Registries (KIM? or OpenRegistry? or …?)

Shared Services: monitoring, audit, instrumentation, standards, APIs, testing & QA, training & support

Hazelton: what is CIFER really?

developing practice of coordination across existing projects in Kuali, I2, Jasig and elsewhere

"More Marketable Open Source Provisioning & Identity Registry" Hazelton, Carter

Carter leads the provisioning and integration workstream of CIFER
Identity Registry is a gap in available open source IdM
Provisioning/Integration integrates systems of record and targets such as LMS, LDAP, AD…

Originally thought of Provisioning as synchronization of registry values to services
Soon realized that these processes parallel the migration of data from systems of record to registry;
thus provisioning is a "wrapper" around the registry.
Subsequent evolution: more than synchronization, some data massage required: maintain consistency, but more than simple synchronization.
Options for provisioning from systems of record:

1. Periodic batch dump to re-create target data; predictable and self-correcting, but latency, only JIC, lots of data to push, no audit!
2. Periodic differential update: calculate changes since last update and apply updates; cheaper, but fragile and still latency, and hard to reconcile with policy/business changes
3. Changelog consumption: record of changes in source system published; reduced (but still some) latency, auditable but somewhat brittle wrt policy changes; sources may not have accessible changelog; "atomic" changes in one system may correspond to composite changes in the other
4. Messaging: source sends messages about changes; near-real time, auditable, more resiliant (with ESB); can do JIT provisioning; brittle under transaction failures (if lose message…); can be expensive to deploy "in the middle"

OpenRegistry (jasig / Rutgers…) ?? and Penn State's Central Person Registry

Open Source Registries

Registry functions
reconciliation of multiple sources; ID match
produce global ID
organize data into standard representation
identity life cycle management

UC Berkeley in essentially same position as UA: legacy Perl code provisioning and sync from systems of record.
Want to replace and provide modern architecture, near-real-time provisioning.
Populate separate Kerberos, LDAP, and AD servers. New unified architecture to be shared by UC Berkeley and UCSF!

Kuali Rice includes KIM Kuali IdM for shared IAM services among all Kuali applications (except Ready!); can integrate with LDAP or other identity stores.

Kuali intends to work with CIFER to standardize APIs and allow Kuali deployers to utilize other CIFER components.
Identity Registries are the first area of concentration.

Identity Registry Group within Kuali
develop document and exercise standard APIs for interacting with regisries
eval Pen States CPR, OpenRegistry, and KIM: OR and CPR are well-developed and comprehensive identity registry solutions; both are viable candidates. KIM more of an integration platform and does not implement all of the functions of identity registry. Likely to go forward with parallel dev. CPR acts as source of identities, creating identifiers, etc., while OR is designed to consume from SoR. CPR $2.7M, OR $1M invested; neither "going away" though adoption (market) may ultimately select a "winner."

Next steps: work on shared APIs
get OR out of incubation status
work with PSU to get to fully open source CPR
UC doing architecture evaluations
inviting other institutions to get engaged in registry work!

Detailed evaluations of 3 registries at spaces.internet2.edu/x/BJ2KAQ