Intellectual Property Policy Reminder: https://www.internet2.edu/policies/internet2-intellectual-property-policy/

Next meeting, Wednesday, July 26 2023, 3:00 PM Eastern

InCommon PeopleSoft Integration Working Group (part of the InCommon Trusted Access Platform)

- ZOOM web conference (first URL doesn't require entering a password)
  - https://internet2.zoom.us/j/6785432100?pwd=OWI1b3ZhTWFUVVhPN2IvMjEza2diUT09
  - https://internet2.zoom.us/j/6785432100 Passcode: 351241
- Or by phone: US: +1 646 558 8656 or +1 669 900 6833 Passcode: 351241
  Meeting ID: 678 543 2100
  International numbers available: https://zoom.us/u/d1DCOApkc

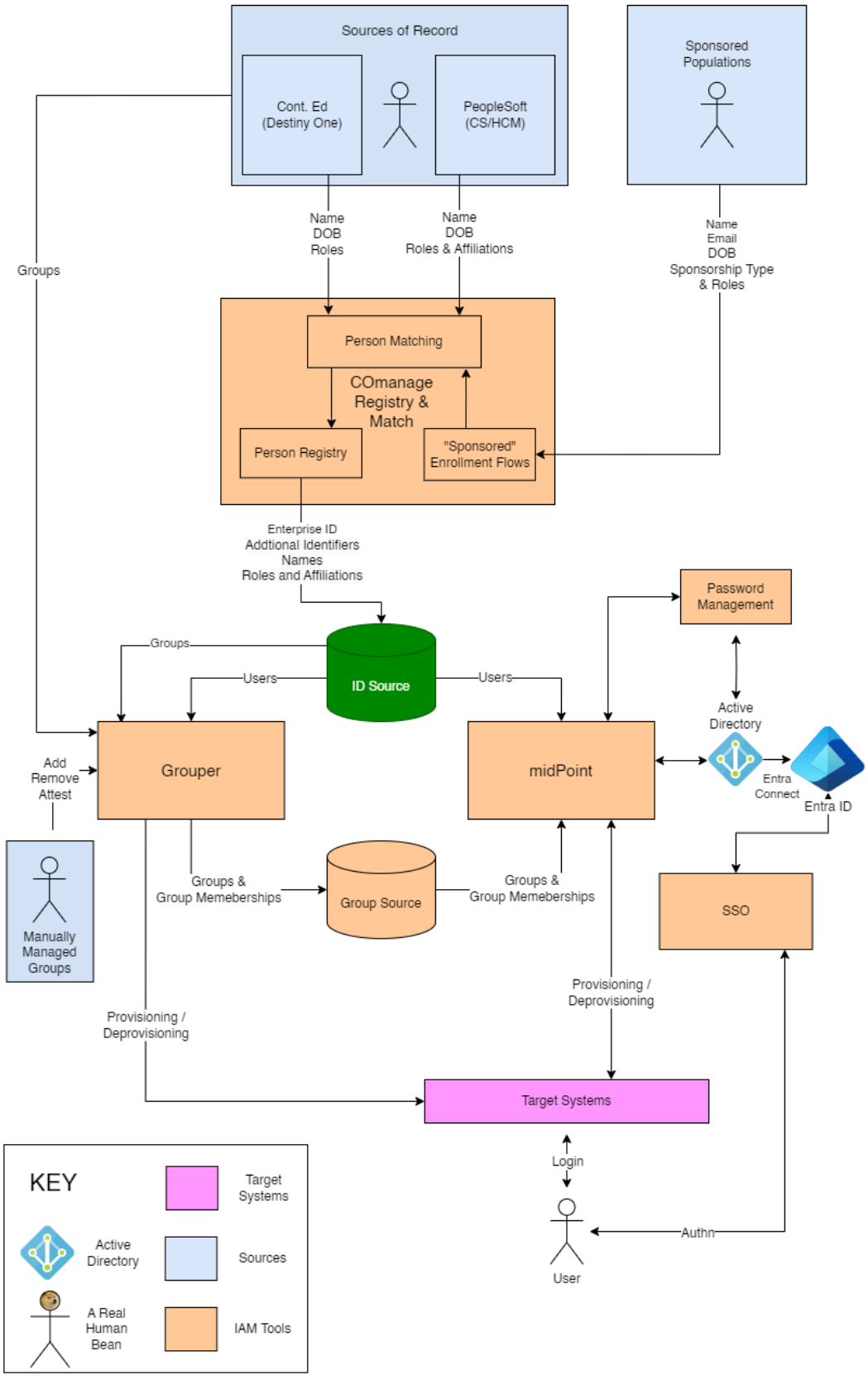
1. SIP: 6785432100@zoomcrc.com

- Or Skype for Business (Lync): https://internet2.zoom.us/skype/6785432100
- This group has an email list midpoint@incommon.org
- This group has a Slack channel, #incommon-midpoint (email help@incommon.org to be added)

Handy Links for the InCommon PeopleSoft Integration Working Group

- Charter
- Wiki Home
- Agendas and Meeting Notes (this document)

IAM Diagram


Sources of Record
Cont. Ed (Destiny One)
PeopleSoft (CS/HCM)
Sponsored Populations
Name DOB Roles
Name DOB Roles & Affiliations
Name Email DOB Sponsorship Type & Roles
Groups
Person Matching
COmanage Registry & Match
Person Registry
"Sponsored" Enrollment Flows
Enterprise ID Addtional Identifiers Names Roles and Affiliations
Password Management
Groups
Users
ID Source
Users
Active Directory
Add Remove Attest
Grouper
midPoint
Entra Connect
Entra ID
Manually Managed Groups
Groups & Group Memeberships
Group Source
Groups & Group Memeberships
SSO
Provisioning / Deprovisioning
Provisioning / Deprovisioning
Target Systems
Login
Authn
User
KEY
Target Systems
Active Directory
Sources
A Real Human Bean
IAM Tools

Friday, March 24, 2023, 10:00 am Eastern, 7 am Pacific, 3 pm London

Participants

1.

Agenda

1. Open microphone. Updates from campuses on plans and integrations.
2. References from previous working group meetings for potential discussion topics:
    a. January 27, 2023: https://docs.google.com/document/d/12UGDAuQ7YlX7szWd4heHyMUaTjPe3HyeWmrF174nQvc/edit#bookmark=id.l180g5l01vx9
    b. September 23, 2022: https://docs.google.com/document/d/12UGDAuQ7YlX7szWd4heHyMUaTjPe3HyeWmrF174nQvc/edit#bookmark=id.sk1gpxmmjeaw

---

Friday, February 24, 2023, 10:00 am Eastern, 7 am Pacific, 3 pm London

Participants

1. Tommy Doan - SMU
2. Keith Hazelton - Internet2
3. Robert Rust - UW-River Falls)\
4. Ethan Kromhout - UNC Chapel Hill
5. Ben Rappleyea - Illinois State University
6. Jeremiah Haywood - Illinois State University
7. David Bickel - Indiana

Agenda

1. Updates from campuses on plans and integrations.

    a. BenR: Getting old groups out of OIM and into Grouper

b. Still sorting out how to handles 2ndary accounts created in AD and then out to LDAP and Student Worker account, admin accounts managed through a request process, will get a separate persona; Will now get entered into midPoint, not final how this will work.
c. TommyD: trying to clarify what an 'admin account' means and how to handle it. Tie it to roles that grant access to needed resources. How to restrict what contexts the student can log into the admin account
d. Robert Rust: ½ to ⅔ of auto-assigned student employee accounts never used, changed to request process
e. When student employees leave their position, their student account automatically goes away
f. BenR: mailing list migration from OIM-managed to Grouper-managed without de-provisioning the OIM account
g. TommyD: Noticing parallels: Cognos, PowerBI, Azure AD, ImageNow also used at SMU
h. JeremiahH: midPoint now in dev, moving to test shortly; Custom web app: A portal that will call out to mP to change passwords, preferred name (must be approved to get into Campus Solutions to avoid embarrassments); RobertR: We have a BP Logix workflow for name changes that creates a ticket when approved; our AD usernames (not UPN) are emplid-based (and our derived student employee and admin accounts are as well)
i. TommyD: Had an issue with Slate: Given names or last names have not been entered into Slate; many left one of them out or entered a period "." Those end up in PeopleSoft. There are cases in which the person has only a single name. Often detected by the wacky email auto-assigned
j. TommyD: Attempting to prevent occurrence of emails with words that overlap with reserved terms by checking against a table. E.g. ftp, ldap, nobody,,, "Offensive" varies by the viewer;
k. DavidB: Do you give people a choice among options for username and email; Avoids these problematic situations. Applicants get an account but then they have to use a separate process to set their email when they show up on campus.

2. Question: What identities do you bring into your person registry? All identities or only ones that have a campus relationship?
    a. TommyD: We follow a 'why not' mindset on bringing 'all' PS people into midPoint. Parents who were former students;
    b. BenR: We brought a million users over from mainframe into PS. We insist that usernames are never reused, so we have to maintain a table to check against when creating a new username
    c. Parent/guardian accounts are assigned and removed by the student. SMU parents don''t get an email account.
    d. TommyD: Do we bring parents in advance into account systems? Or wait until they are assigned an explicit relationship with a student (Just in Case vs Just in Time). SMU has a lot of sponsored account types. SMU Decision log to record the choices made and the discussions around them. See https://www.redhat.com/architect/architecture-decision-records
    e. TommyD: non-credit users in the registry? Yes, we don't want a single user to end u with multiple credentials;
    f. BenR: mP practice: Connect mP to directories: to a single node or… TommyD: Lots of powershell scripts to keep track of which node/domain controller the process started with and stick with that one.

Friday, February 10, 2023, 10:00 am Eastern, 7 am Pacific, 3 pm London

Participants

1. Tommy Doan - SMU
2. Robert Rust - UW River Falls
3. Keith Hazelton - Internet2
4. Pery Doan - SMU
5. Ben Rappleyea - ISU
6. Ethan Kromhout - UNC Chapel Hill
7. Jeremiah Haywood - ISU

Agenda

1. Ben ISU: midPoint is about to take over provisioning to dev instances of PeopleSoft and Active Directory. PeopleSoft work will include profiles, roles, e-consent. Jeremiah is point on the midPoint work. Debezium / Kafka-based solution.

2. SMU engagement with Unicon: Lots of prov targets that we want midPoint to do. PeopleSoft will be among them. Manage HCM through Campus Solutions. Web services planned for mP to Campus Solutions integration

3. API request/response vs message queue: The transport differs although the content of the message and the content of the API response can be the same (JSON is commonly used for both). At SMU, the async side of Integration Broker includes a proprietary messaging system.

4. For Campus Solutions UNC creates a message broker that knows how to talk to PeopleSoft. So the message queue brokers the communication between both sides. It also provides a consistent endpoint regardless of how the integrations may change over time.

Friday, January 27, 2023, 10:00 am Eastern, 7 am Pacific, 3 pm London

Participants

1. Tommy Doan - SMU
2. Keith Hazelton - Internet2
3. Robert Rust - UW River Falls
4. Todd Haddaway - UMBC
5. Pery Doan - SMU
6. Ethan Kromhout - UNC Chapel Hill
7. Jeremiah Haywood - Illinois State University
8. Bill Ewing - University of Texas System

Agenda

1. Revisit working group goals from Sept 23, 2022.

Meeting Notes

Todd: UMBC, what should we do with IAM? Shibboleth and Grouper are solid on our campus. Identity management has a team member leaving next week. Knowledge transfer is pending. Should we move to commercial products or open source? What are others doing? midPoint appears to be maturing.

Bill: UT System. PeopleSoft with Shibboleth for about 10 years. Six campuses share one instance of PeopleSoft. They use the Shibboleth federation discovery service and want to move away from that. How do others integrate PeopleSoft with SSO, particularly allowing multiple IdPs to logon to one Shibboleth SP? Our current attempts are with the Shibboleth Embedded discovery service but we also plan on looking at the Switch wayf.

Jeremiah: Illinois State. They are replacing IAM system with midPoint, and will eventually move to Grouper sending information back to PeopleSoft. PeopleSoft CS generates an identity table that midPoint will read from to get username and identifiers. Will leverage a Kafka queue for that integration.

David: Indiana Univ. Interest in PeopleSoft and midPoint integrations. They currently use Microsoft Identity Manager. Current process pulls in data from HR and SIS from PeopleSoft and then push those out to downstream systems. Currently trying to use two Midpoint setups, one to pull in People from PeopleSoft and build a central “person”. Then another to pull in those people once they have a username in our system to create downstream systems like Azure, Google, etc.

Pery: SMU. Interest in technical details from others on what they are doing.

Robert: UW River Falls. Interest in hearing from others on their integrations. UW has procured Okta but the implementation details are not yet known. They are currently using Microsoft Identity Manager. Their interest is in provisioning as they look to potentially utilize Okta’s identity management tools to replace MIM.

Keith: Internet2. He and others are interested in documenting our meetings in a searchable and summarized form. Here's a link to a draft example from Pery's December presentation on the Affiliation Framework at SMU. Work in progress, but the 1st couple pages should give an idea of what we're aiming for::
iam-knowledge-bits/perydAffilFwork.adoc at 434312261ae9614e4a4c235b4c634174e19a78c4 · internet2/iam-knowledge-bits · GitHub

Tommy: High-level diagrams from campuses to organize the material we're collecting. SMU: PS to person registry, both Grouper and COmanage connected to that registry. Working with Unicon on the design and building.

Friday, December 2, 2022, 10:00 am Eastern, 7 am Pacific, 3 pm London

Participants

1. Robert Rust (UW-River Falls)
2. Keith Hazelton - Internet2.edu
3. Kevin Eder - Indiana University
4. Pery Doan - SMU
5. Tommy Doan - SMU
6. Ben Rappleyea - Illinois State U
7. Mike Dargetz - Illinois State U
8. Ryan Grahs - Illinois State U
9. Geethani Gunasera - Illinois State U
10. Laxmi Malladi - Illinois State U
11. Heather Gwin - Illinois State U?
12. Krista Gaff - Illinois State U?
13.

14. Bill Kaufman - Internet2
15. Janet -
16. Vetrivel - UNC, Chapel Hill

Agenda

Affiliation Framework at SMU (Pery Doan)

Meeting Notes

Affiliation Framework at SMU (Pery Doan)

1. Access Maintenance Automation (Identity consolidation system) is the current service provisioning system targeted to be replaced by the Internet2 TAP components
2. Affiliation == User Type
3. Affil Framework is under Constituent Web Services
4. Multiple efforts on data quality (timeliness and accuracy)
5. CS Affiliation Developer Handbook
6. How long did this take? Consultant in June, went live end of November (last week)

Friday, November 4, 2022, 10:00 am Eastern, 7 am Pacific, 3 pm London

Participants

1. Tommy Doan - SMU
2. Robert Rust - UW-River Falls
3. Tom Jordan - UW-Madison
4. Pery Doan - SMU
5. Benjamin Rappleyea - Illinois State University
6. Keith Hazelton - Internet2
7. Ethan Kromhout - UNC Chapel Hill
8. Bill Kaufman - Internet2

Agenda

1. **Tom Jordan from University of Wisconsin - Madison** will join us to give a broad overview of how they use PeopleSoft integrations for IAM processes, and whatever interesting plans they may have.

2. Look for PeopleSoft developer volunteers to present on any one of several PeopleSoft-related technologies:
    a. Using Person Basic Sync to synchronize person data between modules
    b. Affiliation Framework
    c. Slate integrations
    d. Profile and role management strategies
    e. Common schema elements in PeopleSoft person representations

Meeting Notes

1. TomJ: PeopleSoft HCM to multiple UW campuses' Campus Solutions
    a. One use of Grouper (downstream from above) is to produce service eligibility groups
    b. Nightly full sync: job changes processed only nightly to avoid churn in termination/reinstatement
    c. Workday to Amazon RedShift; Joint data virtualization between analytics and operational data
    d. Campus Solutions will stay
    e. PS delivered integration between HCM and Solutions? No, no common Campus Solution data repositories
    f. See Gartner's 4 styles (levels of maturity) for MDM:
        i. Post-entry matching / reconciliation in Identity Registry
        ii. Centralized: PS search-match (not seen in higher ed)
    g. midPoint complements AzureAD–based provisioning by working for on-campus web applications
    h. Considering COmanage? No. The size of the existing infrastructure makes it impractical to shift. Our direction is to move toward Person MDM. *The realm of person MDM is broader than identity and access management*; A major effort to mature their Data Management; Working on a core

person data model and integrated data governance; Pulling person matching, identity resolution out of identity registry and using golden data concepts from the market; Working with campus–wide data workflows.

i. Motivation for the move from HCM to Workday? Largely driven by business rather than IT. Well-supported cloud environment, a few other nifty features for IAM; Workday represents a different organizational model; from UDDS (parseable) Moving to Workday which supports multiple organizational hierarchies: budget, supervisor, academic. A worthy, but painful, direction.
j. Pery: Thanks for sharing your valuable experience and insights, Tom.

Friday, September 23, 2022, 10:00 am Eastern, 7 am Pacific, 3 pm London

Participants

1. Tommy Doan - SMU
2. Keith Hazelton - Internet2
3. Andrew Parmer - University of Florida (transitioning to UW-Madison)
4. Thomas Carter - University of Florida
5. Heather Gwinn - Indiana University
6. David Bickel - Indiana
7. Pery Doan - SMU
8. Robert Rust - UW-River Falls
9. Ethan Kromhout - UNC Chapel Hill
10. Ben Rappleyea - Illinois State University
11. Jeremiah Haywood - Illinois State University

Regrets: Bill Kaufman

Agenda

What are some reasonable goals for this working group to choose from going forward?

- Focus on key issues/decisions and provide guidance on options
- Invite campus PS SMEs to join calls on specific topics announced in advance
- Hear more about PS *Person Basic Sync* (covers most(?) bio-demo data)
- Hear more about PS *affiliation framework*
- Invite Chris Hyzer to discuss use of org and ref trees for PS in Grouper
- ConnID framework connector boilerplate (db table, messaging)
- Guide to provisioning options for a common set of applications
- ID common schema elements in PS person representations

- Follow-on common elements of Slate integrations

…

Meeting Notes

1. Common/Best practices are elusive, there are as many variants as campuses; Not practical to aim for prescriptive guidance–variety is the rule.

2. We can list things to consider when developing PS integrations

3. Robert Rust: Mode of integration: Triggers on tables, Batch,...; How do sites reduce time from admission to access to apps and resources

4. PeryD: Use case commonality: Maybe list them and reflect on issues and approaches; We've done "Here's where we are"; but what about "What we're headed towards", not a cookbook, but annotated examples; TommyD: How do we capture and present this information.; Pery: A template with a column per campus

5. Focus on key issues/decisions and provide guidance on options

6. RobertR: Also capture pros and cons of a given solution; I'm in the position that in a few years we have to overhaul our IAM

7. PeryD: Foremost audience is those of us on these calls but there other PS schools; Alliance had only a handful of presentations on integrating PS with IAM; General lack of resources. Presentation for next alliance in March 2023; Pery and Tommy would draft something; Bring other campuses into it. Illinois State U. might present on Grouper as role mgmt. Solution. The HEUG puts on the Alliance conference; First past-pandemic and numbers were down.Robert Rust: UWRF attends; Ben Rappleyea: We're mid-journey, so we couldn't present results, but we could present Work In Progress. Ill State U: 21k undergrad, 3-4k grad students (2x SMU)

8. PeryD: Other people might be able to get code samples from us in a few years: Roles, User Profiles are still a bit fuzzy.

9. Ethan: UNC will still be in planning stages: replace BioDemo, HR, Finance into midPoint.a PS to Grouper by March;

10. TommyD: In a few years, there will be a fresh cohort of campuses facing PS integration challenges

11. Invite campus PS SMEs to join calls on key topics; SMU will be able to present on COmanage, Affiliation mgmt. Approaching end of Grouper integration presentations: DavidB, Indiana; Andrew Parmer, moving to UW-Madison starting mid-October, Thomas Carter will stand in for Andrew in presenting U Fl. Tom Jordan seems open to 'presenting' (maybe with PS SMEs)

12. Hear more about PS *Person Basic Sync* web services (covers most(?) Bio/Demo elements; HCM, Fin, Campus Solutions: bio-demo data) Constituent services (yuck?) BenR: PBS pushes to OIM, can shift to other targets. Leverages message triggers handler with enhancement to populate the table, compare that approach with one based on PS Audit; Audit tables are custom, changes are captured. Why don't we have DB triggers?; Pery: Still thinking through it. Hard part is that you'd have to replicate the subscribing node code per PS module

13. Hear more about PS *affiliation framework* lives in Campus Solutions; brings over workforce sync: captures changes there as well. BenR: Us too. EthanK: New to me. Connecting directly to HCM.

14. A topic to explore: How are people integrating/synchronizing data within PS itself between modules such as Campus Solutions, HCM, Financials, etc.; User profiles in Campus Solutions are another source that can sync across modules. TommyD: Plan a rich agenda, schedule a call w PS Devs (with heads–up to PS Devs); BenR to coordinate ISU, Ethan will figure out which devs to invite.

15. Invite Chris Hyzer to discuss use of org and ref trees for PS in Grouper

16. ConnID framework connector boilerplate (db table, messaging)

17. Guide to provisioning options for a common set of applications

18. Common elements of Slate integrations

19. What situations are we targeting with these deliverables?

Meeting Chat:

Agenda:
https://docs.google.com/document/d/12UGDAuQ7YlX7szWd4heHyMUaTjPe3HyeWmrF174nQvc/edit

Pery Doan
https://www.alliance-conference.com/p/cm/ld/fid=212

Robert Rust
welcome to the UW System Andrew!

Ben Rappleyea (Illinois State University)
I feel like we use person basic sync for messages to the table but... again... I am not a PS dev... :(

Tommy Doan / SMU
Ben, would you be able to persuade a PeopleSoft developer involved in that to speak with us?

Ben Rappleyea
Absolutely, have joined in the past occasionally but if we have something specific we want to ask them I am sure I can arrange it :)
Tommy Doan
Agenda item 12 seems like a good topic to hear comments from multiple developers.

Friday, September 9, 2022, 10:00 am Eastern, 7 am Pacific, 3 pm London

Participants

1. Tommy Doan - SMU
2. Robert Rust - UWRF
3. Pery Doan - SMU
4. Keith Hazelton - Internet2
5. Andrew Parmer - University of Florida
6. Ethan Kromhout - UNC Chapel Hill
7. Ben Rappleyea - Illinois State
8. Heather Gwinn - Indiana University
9. David Bickel - Indiana University
10. Jeremiah Haywood - Illinois State

Agenda

1. University of Wisconsin - River Falls (uwrf.edu) PeopleSoft integration story (Robert Rust).

Meeting Notes

1. UWRF overview
    a. 4-500 grad students
    b. Robert Rust there since ‘96
    c. Active in IAM since 2010 during the migration from LDAP to Active Directory
    d. Campus Solutions on prem, HCM managed and provisioned from central UW - Madison

2. Current data flow diagram
    a. System eApp portal will be adjusted to integrate with Slate but not yet
    b. Person data override to ‘correct’ attributes like office number, name coming from SoRs,
    c. Pery: position at SMU is derived from budget data (not really correct source)
    d. Separate DoR db for student employees fed to and managed by MS Identity Manager
    e. ID card db authoritative for identifiers and cards, fed back to AD
    f. Primarily push to AD, but a few provisioning paths out to other apps/services
    g. Which employees are advisers, other relationships handled with simple queries to Campus Solutions that then populate groups in AD;
    h. In 2 separate PS apps: HCM, CampSolutions, integrated via integration broker, each maintains its own EMPLIDs; A job that merges HCM and student info based on

birthdate and SSN matches and feeds in AD; Student EMPLID 7 digits, HCM EMPLID is longer.

i. BenR: HCM drives main identifier processes [check recording]; Not seeing any references to any non-M$ LDAPs yet, do you have any non-M$ LDAPs? If not, do you have "secret" OUs in AD or how do you handle groups that are FERPA protected?
j. RpbertR: we maintain a table of students that have invoked FERPA. In course groups, 80 security groups for course rosters that need access to protected resources.
k. SMU maintains a security group for those who need to access FERPA-protected data

3. Affiliation Calculation
    a. Rules for students; doesn't use affiliation manager
    b. Range of Undergrad vs grad students, stopouts, alums, ;
    c. See table for their current logic for affiliations
    d. Slide 6: sample student attributes
    e. Hoping to stop relying on SSN, shift to alt.email
    f. Slide 7: sample employee attributes
    g. HCM only provides a single work address and phone, doesn't represent multiple roles;
    h. Authoritative source for location? All info comes from PS; PS search/match exclusively relies on de-duplication;
    i. PeryD: Our PS has a lot of dups, RobertR: manual process to mark one EMPLID as 'do not use'; In AD, processes have eliminated dups
    j. BenR: We used to have a LOT of dupes... they are now fewer and further between for sure (now that CS is the source of majority of accounts)

4. Pain Points
    a. No on-prem PS developers, rely on UW-Madison PS staff for development and ops
    b. Complexity arises from PS and campus business logic; New requests require explicit resourcing and prioritization.
    c. Would like to assign lower-level licenses for volunteers, but no source of authoritative data available
    d. Hope to move closer to real-time to maintain current lifecycle state
    e. MIM is a stagnant product, MS focus is now on the Azure product; UWRF has approached them about functionality that Azure lacks.
    f. Intent is to integrate COmanage and Grouper, Robert is their only IAM dev, and that's only 40% of his time.
    g. Single identity across UW System discussed, consultant concluded that data governance concerns made this consolidation impractical;

5. Questions
    a. SMU and UWRF are similarly staffed. Unicon has provided SMU with needed development resources; Tommy: This is what the hope was in forming this group was to provide guidance and documentation that would help modest size campuses be more accurate and specific in their PS integrations

b. PS Shared Services unit at UW has 6-8 devs that UWRF is able to tap into. UWRF is paying for one of these positions.
c. TommyD: Could we persuade one or more of those SMES to join these calls?

Friday, August 26, 2022, 10:00 am Eastern, 7 am Pacific, 3 pm London

Participants

1. Tommy Doan - SMU
2. Andrew Parmer - University of Florida
3. Heather Gwinn - Indiana University
4. Robert Rust - University of Wisconsin-River Falls
5. Todd Haddaway - UMBC
6. Ben Rappleyea - Illinois State University
7. Jeremiah Haywood - Illinois State University
8. Nathan Stien - Illinois State University
9. Pery Doan - SMU
10. Keith Hazelton - Internet2

Agenda

1. University of Maryland Baltimore County (UMBC) PeopleSoft integration story (Todd Haddaway).

Meeting Notes

1. UMBC runs Campus Solutions, Finance, and Human Capital Management

2. Moving to AWS for Campus Portal, Finance
3. Plan to move soon: HCM, Campus Solutions, Gateway
4. On-premises: Campus Solutions, HCM, Grouper, IAM, LDAP
5. Grouper subject source: Emplids, userids, campusId brought into Grouper

HR INTEGRATION:

6. HR going to AWS in a week, Campus Solutions in a month or so
7. Pull from CS and HCM (both are systems of record for identity data) into Grouper.
8. Provision to Google
9. Hooked up Grouper to Duo; to manage fac/staff/ about to add students. Costs will go from $5K to $$$$; Grouper manages 'eligible to use 'Call Me'
10. Emeritus life cycle has been paper-centric and involved lots of staff in the process; Now we select emeritus status from PS, put in an emeritus-service-enabled group. Emeritus designation is made in HCM Job data.
11. Emeritus and retirees affiliation assignments have a 1-year grace period.

CAMPUS SOLUTIONS:

12. Grouper group for recent graduates (60 days post retirement
13. Fac/Staff/Student plus Recent Grads
14. Advisors and financial aid staff belong to a group, pushed to campus portal with a service menus
15. They have one loader job to load all majors.
16. Governance & access policy groups work well because IT is highly centralized and IT has established a strong trust relationship with the functional areas, parceling out the management tasks and policy decisions to the appropriate 'deciders'
17. UMBC is about 3,000 employees, 12,000 UG, 3,000 GR, and 3 on IAM Team.

FUTURE PLANS: More functions for Grouper.

1. Course enrollment loaders,
2. PeopleSoft security (assigning roles)
3. automated PeopleSoft deprovisioning,
4. Campus Portal currently gets data from LDAP so they may move to messaging with Grouper instead (Rabbit MQ),
5. drive LMS with Grouper,
6. door access management (Lenel/S2) with distributed management
7. Todd is a big fan of cloud computing, prefers not to create and manage hybrid architectures.
8. One non–prod Grouper instance; Group design, provisioning is ToddH, Chris does integrations like provisioning hook-ups; Non-prod instance; plus some changes can be

9. Working with Moran to develop strategic directions in IT; 1) Stick w what we have; 2) Go with OS software like midPoint; 3) find commercial solutions for select areas;
10. Cautious about midPoint: Campuses say they're running it, but they aren't putting it at the center of their IAM infrastructure.
11. CS - HCM integration bi-directional;
12. Recruitment is with Salesforce, considering expanding scope of Salesforce
13. Grouper in use for 5 years plus
14. Paul Riddle lobbied to get business logic out of IdP and into Grouper
15. Loader job count: ~75
16. Future discussion: Drifting to the Cloud: ideas, ways, and means

---

Friday, August 12, 2022, 10:00 am Eastern, 7 am Pacific, 3 pm London

Participants

1. Tommy Doan - SMU
2. Keith Hazelton - Internet2
3. Ben Rappleyea - Illinois State U
4. Jeremiah Haywood - Illinois State U
5. Todd Haddaway - UMBC
6. David Bickel - Indiana U
7. Ethan Kromhout - UNC Chapel Hill
8. Robert Rust - UWRF
9. Pery Doan - SMU

Agenda

2. Illinois State University PS integration story (Ben Rappleyea et al.)

Meeting Notes

Illinois State University PS integration story (Ben Rappleyea et al.)

1. Migration from OIM to Grouper for group management (OIM can put people into groups but can't take them out of LDAP.
2. Query for large affiliations fails occasionally (ran but didn't pull all matching records, and OIM then removes the accounts
3. Integration broker, then assign primary affiliations; ISU Email Addr assigned by OIM and sent back to PS campus solutions
4. Future solution: midPoint creates accounts using messaging; Grouper will query HCM and Campus Solutions. Grouper will create the primary affiliation; Starts with a series of memberships, hierarchical membership rules (20 groups) that resolve to primary affiliations
5. Grouper messaging back to Campus Solutions via Debezium to Kafka
    a. Grouper subject source description format:
    b. (username, subjectId) (Active/Inactive) - Primary Affiliation - Title

    c. (rrbird, xxxxxxxxxxx) - (Active) - AFL_CIVIL_SERVICE - IT Tech Assoc
    d. "Debezium is a distributed platform that converts information from your existing databases into event streams, enabling applications to detect, and immediately respond to row-level changes in the databases. Debezium is built on top of Apache Kafka and provides a set of Kafka Connect compatible connectors." – Google search
6. Reducing role of messaging: Eventually only mP to Campus Solutions
7. Integration layer: Red Hat JBOSS; custom groovy for business-relevant calculations;
8. Pery wants to use PS delivered functionality for modifying user profiles.
9. Campus Solutions assigns identifiers, OIM adds UUID

Questions for Ben

1. ULID (University Login ID) is PS OperID; Emplid is different (Pery ours are one and the same); Campus ID is UID, a 9 digit SSN replacement, kept in HCM as "EmplID") should be the primary identifier since ULID is based on names which can change; CS and HCM are integrated; CS generates IDs, HCM does not; EmplID is 10-digit; CampusID and EmplID are immutable (rare exceptions); ULID change requests are reviewed
2. Robert Rust to Everyone: our network logon IDs ("Falcon IDs") are W + 7-digit emplid and our OPRID = network logon ID = sAMAccountName = CN
3. CTM Constituent Transaction Manager is where the business logic, search match, etc. are processed
4. Grouper API is a backup path,

Friday, July 29, 2022, 10:00 am Eastern, 7 am Pacific, 3 pm London

Participants

1. Tommy Doan - SMU
2. Keith Hazelton - Internet2
3. Robert Rust - UWRF
4. Ethan Kromhout - UNC Chapel Hill
5. Bill Kaufman - Internet2
6. Heather Gwinn - Indiana University
7. Pery Doan - SMU
8. Benjamin Rappleyea - Illinois State University
9. Anderson Klay - Illinois State University

Agenda

1. Today we will initiate a series of focus groups, starting with **Grouper integrations with PeopleSoft**. These focus groups are intended to discuss use cases, desired outcomes, integration mechanics, and particularly PeopleSoft-related configuration details. Discussion about the value of the Grouper integration is helpful! Presentation material is not required but certainly welcome.
   Volunteers for conversations about what other campuses are doing are welcome for future meetings. Ethan Kromhout from UNC Chapel Hill will provide the first conversation.

Meeting Notes

1. Initiate a series of focus groups meeting; Grouper 1st, then midPoint, then COmanage. Open to feedback from all of you
2. Ethan on UNC: 3 main paths for PS - Grouper

a. Dir Mgr: Home grown Java app takes data to LDAP and AD; Messages and SOAP Web Services; Polling worked well, so added SOAP; both achieve near-real time currency.
    i. Triggers on bio-demo tables on Campus Solutions and on student status records pushed to LDAP; Msg sent to Integration Broker (IB); A JMS adapter on IB
    ii. HCM and Finance: SOAP queries for jobs, sponsored researchers, contractors through our affiliate system. One simple query to finance just for Department names (and numbers)

    iii. Dir Mgr has its own LDAP and that gets replicated to OpenLDAP; Grouper gets its subject source and affiliation info via LDAP
        1. PS queries Grouper for courses and rosters with roles; published out to O365; Sakai for majority of classes, migrating some to Canvas
    iv. PS Portal is also in use

    v. Informatica (ETL tool) So PS and other devs can write queries to populate databases and provide access via APIs. Many developers opt for daily or other scheduled updates
    vi. SQL queries to PS towers; Push to Grouper via Grouper WS's. PS sec folks want Grouper to represent the PS role tables; Also things like HIPAA org membership; All published to Grouper, many get passed on to OpenLDAP

b. Dozens of Grouper loader jobs, 3 - 4 times a day, go against PS internal db tables
c. Once its in Grouper, what's the rest of the provisioning story: EK: We do use attributes to specify which groups get provisioned where; Grouper keeps track of primary affiliation querying itself; Majority of provisioning happens via midPoint using delivered Grouper-midPoint integration; Broad affiliations: student, faculty, member: Determined by DirMgr, reflected to Grouper then leveraged by Shib for attribute assertions; No prov back to PS; People will have Emplid and attributes, PS login identity used to generate OperId; Future: Push OperID as soon as NetID is created; Big question marks: Like to move away from msg and SOAP since thos are all locally built and maintained; can we slowly move to delivered PS services for integration with Grouper;
d. Pery: PersonBasicSync: tried that attractive approach to integrate with 3rd parties; SMU will create a custom web service to be driven by PersonBasicSync; Ethan: OIM uses Constituent Sync; BenR: ConstSync is not reliable; Future: Message will populate a table that mP reads. View and recipient changes get reflected to the table that mP queries;
e. JMS, RabbitMQ: No real cases of messages being lost; clustered services, messages saved to disk. Stops rather than losing messages. BenR: Table reads are faster than message processing; Ethan: Is all of the DB provisioning stuff in Grouper in there? BenR: Yes, with Grouper 2.6.9; Drew has Shib working with 2.6.9; BenR: Table is
f. reconstituted by Grouper if the table gets blown away. Ethan: mP ability to get Grouper current state with the DB in the middle;

g. Pery: Ethan: what's your future state? EK: 1) move biz logic out of local DirMgr to Grouper to make it easier to see how people get the provisions; mP direct link to PS; OpenLDAP will remain as Grouper subject source, and management will shift over to midPoint; Published affils in LDAP today calc'd by DirMgr, shift to using Grouper and write back to OpenLDAP.
h. TD: Our idea has been PS would be responsible for computing high-level affiliations (student, employee (current, former); anything more granular would be done in Grouper; Ethan: Former employee is read directly from PS; Student definition is more complex, so DirMgr takes care of that (and Grouper will take over)
i. DirMgr existed long before PS came to campus, so DirMgr did all the munging to produce the information that the UNC apps needed.
j. Slate? Only sent from CS after students are admitted; Fees paid, etc. Nearly universal, esp. With PS.
k. Robert Rust: out of curiosity ... how would someone handle affiliations that change based on a date that PeopleSoft is the SOA for? For example, someone changing to a current student when a term changes (which doesn't necessarily affect something on the student's record) (in the case where Grouper is deciding on affiliation); Queries back to PS for that kind of info;
l. PeryD: Affiliation Framework report in August; TD: We do make significant use of Affiiliation Framework.

Friday, July 15, 2022, 10:00 am Eastern, 7 am Pacific, 3 pm London

Participants

1. Tommy Doan - SMU
2. Robert Rust - UWRF
3. Pery Doan - SMU
4. Ethan Kromhout - UNC Chapel Hill
5. Keith Hazelton - Internet2
6. Benjamin Rappleyea - Illinois State University
7.

Agenda

2. Today we initiate a series of focus groups, starting with **Grouper integrations with PeopleSoft**. These focus groups are intended to discuss use cases, desired outcomes, integration mechanics, and particularly PeopleSoft-related configuration details. Discussion about the value of the Grouper integration is helpful! Presentation material is not required but certainly welcome.
   Volunteers for conversations about what other campuses are doing are welcome for future meetings. Ethan Kromhout from UNC Chapel Hill will provide the first conversation.

Meeting Notes

1. We may delay the UNC discussion today since we have low attendance. Pery suggested we send a note to the distribution and to the Slack channel to make everyone aware of our agenda prior to our meetings. Tommy and Keith will discuss.
2. Keith: Anyone planning to use ConnID with midPoint to PeopleSoft? Ethan, yes UNC plans to do so. Moving to Provision IAM's (formerly !Labs) Base connector would be pretty disruptive to what their development team is already doing. Evolveum has a developer guide for ConnID. ConnId 1.x Connector Development Guide - Evolveum Docs

Friday, July 1, 2022, 10:00 am Eastern, 7 am Pacific, 3 pm London

Participants

8. Tommy Doan - SMU
9. Keith Hazelton - Internet2
10. Benjamin Rappleyea - Illinois State University
11. Jeremiah Haywood - Illinois State University
12. Pery Doan - SMU
13. Robert Rust - University of Wisconsin-River Falls
14. David Bickel - Indiana University
15. Ethan Kromhout - UNC Chapel Hill
16. Jeffrey Crawford - UCLA

Agenda

3. Discussion about moving the direction of the working group to a series of focus groups.
    a. Grouper integrations
    b. midPoint integrations
    c. COmanage integrations

Friday, May 20, 2022, 10:00 am Eastern, 7 am Pacific, 3 pm London

Participants

1. Tommy Doan - SMU
2. Bill Kaufman - Internet2
3. Keith Hazelton - Internet2
4. Robert Rust - University of Wisconsin-River Falls
5. Ethan Kromhout - UNC Chapel Hill
6. Shumin Li - University of North Carolina Chapel Hill
7. Pery Doan - SMU
8. Nathan Stien - Illinois State University
9. Heather Gwinn - Indiana
10. David Bickel - Indiana
11. Anderson Klay - Illinois State University
12. Jeremiah Haywood - Illinois State University
13. Ben Rappleyea - Illinois State University

Meeting Notes

1. All invited to look at the existing questions (below), add questions you think might be good to add. Comments or questions are invited as well

    a. Keep in mind that this will be circulated to PS Higher Ed Users Group (HEUG) and that group may not be as deep into IAM, so include some questions that make fewer assumptions about
    b. An ongoing stream of access changes (adding and removing permissions) are driven by lifecycle transitions in a person's relationship to the institution; how is this managed?

Survey questions:
An Internet2 working group is gathering experiences and plans from university campuses where PeopleSoft is in use. This survey seeks to gather an expression of interest from any campuses that involve PeopleSoft data in their Identity and Access Management (IAM) solutions.
For purposes of this survey, IAM systems involve a **person registry**, an **access management system**, and a **service provisioning system**. If your campus integrates or wishes to integrate PeopleSoft with any such systems, please complete the survey! Based on your responses, the working group may follow up with you to conduct an "interview" to gather technical details.

Some definitions:

- Internet2 is a community providing a secure high-speed network, cloud solutions, research support, and services tailored for research and education. Our community includes higher education, research institutions, government entities, corporations and cultural organizations. Through InCommon, Internet2 provides security, privacy, and IAM tools built for research and education.
- **Person registry**:
    - a unified view of people who are or have been authorized to interact with managed systems
    - repository that establishes a person's identity with unique identifier(s) and stores bio/demo data about them
- **Access management system**: a system of managing appropriate access to resources; adding and removing rights and permissions.
- **Service provisioning system**: a system designed to actually make resources available to authorized users in a timely manner (productivity-focus), and also remove them in a timely manner (security-focus).

Initial Survey

1. PeopleTools version(s)
2. PeopleSoft applications used
    a. Campus Solutions (CS)
    b. Human Capital Management (HCM)
    c. Customer Relationship Management (CRM)
    d. Other
3. Does your institution have an Identity and Access Management (IAM) system (a system of managing appropriate access to resources similar to Person Data in PeopleSoft)?
    a. Yes, custom bolt-on within PeopleSoft
    b. Yes, homegrown application outside of PeopleSoft
    c. Yes, commercial product that integrates with PeopleSoft
    d. Yes, open source product that integrates with PeopleSoft
    e. No
    f. Other

Person Registry integration questions

4. What does your institution use as its Person Registry (repository that establishes a person's identity with unique identifier(s) and stores bio/demo data about them)?
    a. PeopleSoft Campus Solutions
    b. PeopleSoft HCM
    c. PeopleSoft CRM
    d. Custom bolt-on within PeopleSoft
    e. Homegrown application outside of PeopleSoft
    f. Commercial product outside of PeopleSoft
    g. Open source product outside of PeopleSoft
    h. I'm not familiar a Person Registry
    i. Other?
5. Does your Person Registry include non-employee/non-student identities (i.e. guests, contractors, sponsored)
    a. Yes
    b. No
    c. Not yet
    d. Maybe
    e. Other
6. Where do you assign relationships with your institution for your PeopleSoft identities?
    a. In PeopleSoft CS Relationship with Institution Legacy Table
    b. In PeopleSoft CS Affiliations Framework
    c. In PeopleSoft HCM Organizational Relationships
    d. In PeopleSoft custom bolt-on
    e. Outside of PeopleSoft
    f. Other
7. If using an external Person Registry, how is it kept up to date with changes in PeopleSoft?
    a. File-based updates
    b. DB links/SQL direct
    c. Rest API
    d. Synchronous/Asynchronous web service
    e. Messaging such as Kafka, JMS, or AMQP
    f. Some combination
    g. Other
8. What is the timing of communicating changes in Peoplesoft identity data to consuming systems?
    a. Near real time
    b. Batch updates
    c. Mix of both

Provisioning integration questions

9. How do you provision user profiles for new users (students or employees) into PeopleSoft?
    a. PeopleSoft CS New User Registration
    b. Custom bolt-on
    c. Automatically through IAM provisioning system
    d. Manually
    e. Other
10. How do you manage (assign/remove) default and/or administrative PeopleSoft roles?
    a. PeopleSoft Dynamic Role Rules
    b. Custom bolt-on
    c. Automatically through IAM provisioning system
    d. Manually
    e. Combination of automated and manual
    f. Other
11. How do you de-provision user profiles for offboarding users?
    a. Custom bolt-on
    b. Automatically through IAM provisioning system
    c. Manually
    d. Other
12. How do you modify role assignments based on changes in user relationships/active positions within the organization?
    a. Automatically through IAM provisioning system
    b. Manually
    c. Combination of automated and manual
    d. Other

Access management system integration questions (providing and revoking the rights that people have in different systems)

13. What data do you bring from PeopleSoft into your access management system?
14. What do you attempt to do with access management based on PeopleSoft data?

Solicit further involvement

15. Would you be interested in participating further by meeting with a few members of the working group so we can gather additional details about your IAM architecture, with special emphasis on the PeopleSoft integrations?
    a. Yes
    b. No
    c. Maybe
    d. Other
16. Do you plan to work with a consultant or partner on redesigning or enhancing your IAM integrations?

17. How would you rate your satisfaction with your current PeopleSoft integrations?
    a. We would like to scrap it completely
    b. We have many pain points which cause a lot of work
    c. It works okay most of the time
    d. We have very few complaints, just the occasional issue
    e. It is working well and can be a model for others

Interview from Outline:

- Ask more specific questions about PeopleSoft delivered functionality and customer satisfaction, some examples:
    - Search/Match
    - CTM
    - Affiliations Framework
    - New User Registration
    - Dynamic Security
- PS to Identity Registry: Initial import of identity data into the Identity Registry
    - This assumes an external registry - adjust as above
    -

- Deriving access management information from ‘raw’ Peoplesoft data fields
    - Where is this done?
    - What role, if any, does Grouper play?
    - Other Product(s)?
    - Affiliations and roles
    - Document as schema mappings or list key PS attributes that are used to develop groups for AuthZ
    -

- Registry functions?
    - Matching (PS has a search-match tool)
        - Search-match Rules used?
            - more details about this
        - External Match functions?
    - Other SORs (separate SIS?)
    -

- Data flows back into PeopleSoft - Provisioning back
    - Managing PS operator privileges
    - Identifier mappings
    - Role assignments
        -
    -

- Architecture diagrams
    -

Friday, May 6, 2022, 10:00 am Eastern, 7 am Pacific, 3 pm London

Participants

1. Tommy Doan - SMU
2. Keith Hazelton - Internet2
3. Pery Doan - SMU
4. Bill Kaufman - Internet2
5. David Bickel - Indiana
6. Shumin Li - University of North Carolina Chapel Hill
7. Jeremiah Haywood - Illinois State University
8. Ben Rappleya - Illinois State University
9. Majeed Abu-Qulbain - Illinois State University
10. Jeffrey Crawford - UCLA
11. Robert Rust -

Agenda

1. Proposal: Small groups of campuses that share an integration challenge: Grouper prov, midPoint prov, COmanage prov.
    a. DavidB, Indiana: We'll want to integrate all 3: PS, mP, COmanage
    b. RobertR,
2. [Keith] Reach out to Banner WG members to recruit

Survey Link (the goal is to collect integration patterns from folks to find common working practices to help develop recommendation, recipes, and how to's

- Suggestion to make some of these multiple choice questions
- PeopleTools version
- What PeopleSoft modules are in use?
- Other questions:
    - Do you use PeopleSoft as the registry?
    - If not what product(s) do you use for your campus People Registry?
    - TAG Categories?
        - Registry
        - Access Management
        - Data Flows into PS - Provisioning back to PS
        - General Architecture (Diagrams)
- There is a PS Alliance conference annually - perhaps use this list to reach out to
    - Higher Education User Group (HEUG) https://www.heug.org/resources/heugrecentblogs

    - 900 institutions from 30 + countries
- See if UW Madison would be willing to share their PS implementation
- JeffC: UCLA - Use Grouper and loader integrated with PS data
    - Create groups with Empl Class, Job Code, Department, Status (active, terminated (keep for last 30 days) etc) - Took time to derive the most important classes
    - Since 2016 - but integration with PS was toward latter 2018
    - Pulling the PS data into loader jobs is still evolving
    - VPN's is a strong Use Case
    - UI starting to use Grouper threshold features
        - groups that are small with minimal churn treated differently than large groups with frequent changes
    - UNC Chapel Hill: using threshold to mitigate database disconnect errors so that key data is not accidentally deleted
        - Populate PS Org data into LDAP and Grouper pulls from LDAP
        - IU has a similar pattern
    - Illinois State Planned Architecture Diagram: https://photos.google.com/share/AF1QipPbKtibWotmdZFamXza8RYrSdx0DTpk4Lx7gXLkuZR5Q4bR3TBvRi-LGNzY7HFGzg?key=WTFJcTFldWVLNGpxakxIWlJxWEkyMi1LTzh4MkZB
    - Illinois State: Using midPoint to DB table then have a KAFKA integration to write back to PS WebServices
        - GAP around doing a full reconciliation. midPoint can do a reconciliation with the DB table but does not have a full view of PS data
    - UNC does not write data back to PS currently. using midPoint to do various types of synchronization

Initial Survey Outline:

- PS to Identity Registry: Initial import of identity data into the Identity Registry
    - This assumes an external registry - adjust as above
- Keeping Identity Registry up to date with changes in PeopleSoft
    - File based
    - API
    - SQL direct
    - Messaging
    - Some combination
    - Other
    - Registry functions?
        - Matching (PS has a search-match tool)
            - Search-match Rules used?
                - more details about this
            - External Match functions?

        - Other SORs (separate SIS?)
- Deriving access management information from ‘raw’ Peoplesoft data fields
    - Where is this done?
    - What role, if any, does Grouper play?
    - Other Product(s)?
    - Affiliations and roles
    - Document as schema mappings or list key PS attributes that are used to develop groups for AuthZ
    -

- Data flows back into PeopleSoft - Provisioning back
    - Managing PS operator privileges
    - Identifier mappings
    - Role assignments
        -

- Architecture diagrams

Friday, April 22, 2022, 10:00 am Eastern, 7 am Pacific, 3 pm London

Participants

1. Tommy Doan - SMU
2. Keith Hazelton - Internet2
3. Ethan Kromhout - UNC Chapel Hill
4. Robert Rust - UW-River Falls
5. Pery Doan - SMU
6. Todd Haddaway - UMBC
7. Jeremiah Haywood - Illinois State University
8. David Bickel - Indiana
9. Bill Kaufman - Internet2
10. Benjamin Rappleyea - Illinois State University
11. Andrew Parmer - University of Florida

Agenda

1. PS Integration Interviews (TAP components and other integration targets)
    a. Individual or public
    b. Bring PS

2. Seeking Initial Volunteers for the following rough survey
    a. Todd, UMBC to be scheduled
    b. Ethan, yes, down the road; Legacy integration and Grouper, Cirrus Identity, Shib.
    c. BillK: Templatize these questions? (on the wiki)
    d. Email from Netta yesterday: bringing the WGs together
    Cheers to InCommon Volunteers! 6 Ways You Made Us Proud in 2021 - InCommon
3. Integrations COmanage, midPoint, Grouper; But also Shibboleth (or another WebSSO integration)
4. Sharing integration stories but invite comments; Todd: Fronted WebLogic with Apache; Robert Rust: We're using the same: WebLogic proxy fronted by Apache. There's curiosity out there about whether a site is doing it the "right" way or "best" way. TommyD: We have IIS as proxy; So this group can provide material that would help;
5. TommyD: Detailed document on our wiki about how we do it, with some sanitization, could be shared
6. PS/Shib integration needed participation of PS specialists, not just Shib experts.
7. Jeremiah: Plans for integration of mP to pass info back to PS. Postgres replication based on a message queue; e-consent, email address, role data information back to PS.

Survey Outline:

- PS to Identity Registry: Initial import of identity data into the Identity Registry
    -
- Keeping Identity Registry up to date with changes in PeopleSoft
    -
- Deriving access management information from ‘raw’ Peoplesoft data fields
    - Where is this done? What role, if any, does Grouper play?
    - Affiliations and roles
    - Document as schema mappings

- Data flows back into PeopleSoft
    - Managing PS operator privileges
    - Identifier mappings

- Architecture diagrams

InCommon Accomplishments - Q1 2022

Key Topics of Discussion/Projects	This working group was requested and approved by CACTI and had its first meeting on Jan 14, 2022
Kudos	Thanks to Tommy Doan of SMU for volunteering to chair this group. He will be assisted by Keith Hazelton (consultant to Internet2) and Ethan Kromhout (UNC Chapel Hill)
Community Hours of Work	87

Friday, April 8, 2022, 10:00 am Eastern, 7 am Pacific, 3 pm London

Participants

1. Tommy Doan - SMU
2. Keith Hazelton - Internet2
3. Bill Kaufman - Internet2
4. Ethan Kromhout - UNC Chapel Hill
5. Todd Haddaway - UMBC
6. Pery Doan - SMU
7. David Bickel - Indiana University

8. Andrew Parmer - UFL
9. Chris Sutherin - UMBC

Agenda

A plan for documenting the variety of existing PeopleSoft integration solutions: An environmental scan

Once we begin to collect and document these artifacts they will be added to the wiki for easy reference as a starting point.

1. PS to Identity Registry: Initial import of identity data into the Identity Registry

2. Keeping Identity Registry up to date with changes in PeopleSoft

3. Deriving access management information from ‘raw’ Peoplesoft data fields
    a. Where is this done? What role, if any, does Grouper play?
    b. Affiliations and roles
    c. Document as schema mappings

4. Data flows back into PeopleSoft
    a. Managing PS operator privileges
    b. Identifier mappings

5. Architecture diagrams

Seeking volunteers for interviews: Option to conduct privately or with the full team: Florida, Indiana, UNC, SMU, UMBC

ToddH: Send out a survey to get a broader sample of responses; Introduced Chris Sutherin: PS Admin, DBA, Grouper SME, Containerization architect; could help formulate

BillK: Start the survey with the members of this group, review what comes in and then do a broader survey

Ethan: TAP integration only? No, we are interested in PS Integrations regardless of Registry choice.

Also want to hear from those currently planning their integration

ToddH: Encourage PS Developers to participate as SMEs; TommyD: Pery is the PS developer from SMU attending these calls;

TommyD: Interest in PS Affiliation Framework: Delivered Oracle service to help determine what relevant affiliations are and; Pery: Leverage application so we can run batch process; AF can set triggers to capture

changes; Some data changes are not captured with triggers, but if a batch approach can detect deltas, that would complement trigger-based data change prop; Queries db to detect changes (part of the Affiliation Framework delivered functionality); TommyD: Knows of another campus that is interested; Ethan's interested in the Affil. Framework; Tommy: May only be of interest to site that are working with an Identity Registry;

Pery: Custom bolt-on AMA that currently computes affiliations; Example: providing services to new employees before they are entered into HR ERP. Constituent Services web services are not ideal, but they can help capture changes, and combined with Affiliation Framework allow us to piggyback on those triggers to publish our own custom messages.

David Bickel: We use Grouper to do a lot of this affiliation management. Custom queries now, but use Grouper loaders to do this; Use TAP components to perform identity and access functions even before they are brought into PeopleSoft. Tommy: What you're talking about is very familiar in terms of person registry (COmanage, midPoint)

Chris: Grouper in prod at UMBC, use will expand from current scope Provisioning to Google, mailing lists: Deciding on overall IAM direction, Moran Tech is being brought in to recommend an IAM Strategic Plan; Todd: Affiliations assigned with home-grown code; PS passes info down that factors into their coarse-grained privileges (students get X, faculty get Y); Use Grouper to increase granularity of service access.

TommyD: We had a consultant in 2018-2019, couldn't afford to follow their recommendations, so turned to TAP. Grouper manages service eligibility, midPoint to 'make it so' through provisioning; Using components for their core strengths

Before next meeting: A volunteer that agrees to be first, let Keith, Tommy, Bill know. Include a high-level architecture diagram that covers the topics under review.

Friday, March 25, 2022, 10:00 am Eastern, 7 am Pacific, 3 pm London

Participants

1.
2. Tommy Doan - SMU
3. Pery Doan - SMU
4. Robert Rust - University of Wisconsin-River Falls
5. Andrew Parmer - University of Florida
6. Ethan Kromhout - UNC Chapel Hill
7. Todd Haddaway - UMBC
8. Bill Kaufman - Internet2
9. Ben Rappleyea - Illinois State University
10. Keith Hazelton - Internet2
11. Nathan Stien - Illinois State University

Agenda

Open Discussion Today

1. Tommy - thinking about direction of the group

    a. Discussions have revealed that virtually no 2 institutions have very similar patterns in how they currently have PeopleSoft integrated
    b. Robert - current state is not necessarily where we want to be, looking for what direction we want to go. An issue for us is timeliness of Provisioning. Right now he does not have any of the PeopleSoft team involved in the next steps for their IAM development. Would like more guidance on which components to use, best practices, etc.
    c. Todd - working on a cookbook seems like the best way to proceed, did this with Grouper by looking across the published use cases/stories. How to integrate PS with Grouper in a particular pattern (say HR purposes) would be a useful pattern that could help others
    d. Tommy - so collecting and archiving Use Cases that are successful
    e. Todd - that is part of it but then drilling into specific recipes would be useful
    f. Tommy - SMU has a goal of eventually use midPoint to provision to PeopleSoft
    g. Ben - our goal is to get data out of PeopleSoft and into Grouper then back to PeopleSoft
    h. Tommy - so perhaps we have shared experiences about integrating with Grouper but midPoint and COmanage integrations will be more greenfield
    i. Robert - another thing that would be helpful to me would be identifying table triggers that would be useful
    j. Pery - can the working group produce a set of templates where campuses can contribute their use cases and cookbooks.
    k. Bill - a wiki space could be used for that.

l. Ethan - delivered components in PeopleSoft that could be used for retrieving and delivering data. Identify those and enumerate them.
m. Ben - ISU should be able to help with that.
n. Todd - common API related endpoints
o. +1 to Bill's idea: Wiki space for templates for contributions, produce content between calls, review content on the calls.
p. Original idea: work on integration of PS with each TAP component; Some integrations will be of limited interest; PS to Grouper is probably of widest interest; Grouper integration would focus on loader job queries, and wouldn't exercise APIs and other such channels
q. Ethan: Grouper - PS shouldn't be our only focus. Also valuable to have PS - midPoint (#2) and PS - COmanage (#3)
r. TommyD: Still charting our course with this working group
s. BillK: Look to Grouper, for ideas on use cases to be covered for PS, midPoint, and others; call on David Walker to help with editing the material.
t. UW-Madison, Tom Jordan: About to migrate off PS to Workday
u. Andrew Parmer: Affiliation based on PS data U Florida; Home grown processes to pull HR, student data and populate affiliations; Working on midPoint and COmanage;

2. Next steps: plan how to use the already existing wiki space; Right now just has meeting notes, charter; Short planning call to sketch out use of wiki: Bill, Tommy, Ethan, Keith

---

Friday, March 11, 2022, 10:00 am Eastern, 7 am Pacific, 3 pm London

Participants

1. Tommy Doan - SMU (Conflicting meeting today)
2. Keith Hazelton - Internet2
3. Todd Haddaway - UMBC
4. Jeremiah Haywood - Illinois State University
5. Benjamin Rappleyea - Illinois State University

6. Geethani Cabraal - Illinois State University
7. Jeffrey Crawford - UCLA
8. Bill Kaufman - Internet2

Agenda

Continue collecting current practices, picking up from the February 25 meeting

1. What data do you provide **from IAM to PeopleSoft**?
    a. UMBC: CampusID unique id: 2 letters, 5 numbers; login id can change but not often, All system identifiers flow back to PS; Welcome email with link to generate account (user picks a username), email is separate
    b. ISU: LoginID, email, E-Consent (user agrees to use of e-sig) (go back to PS
        i. LoginID can and does change frequently (First initial, Middle initial, first 5 characters of last name or replaced with numbers if ID was unavailable)
    c. (UCLA) PS HR, campus ID, business email, business telephone number; mulesoft for assignment across all campuses
        i. Plans to add livename pushed back to PS, driven by compliance requirements
        ii.
    d.

2. What technology do you use to export the PeopleSoft data for a one-time data conversion export?
    a. ISU: No plans; identity table has the data, PS places into data table that mP loads from
    b. UCLA: Centralized, so there was a down-time conversion, employees brought in by messaging. Similar to how live sync works; Push used same system for daily
    c. UMBC: Use messaging, bulk and incremental use same approach

3. What technology do you use for ongoing synchronization?
    a. UCLA: SOA ESB constructed at system level with Mulesoft licenses; internal systems use queues,
    b. UMBC: PS messaging to push down XML; Informatica may take over all messaging tasks, maybe RabbitMQ
    c. ISU: Homegrown Java-based; Kafka; Different team.

4. What triggers the synchronization?
    a. ISU: in test, mods to user send message to OIM and to the tables (last-updated)

    b. UCLA: HR changes trigger messaging to the affected campus, also send dumps per campus (operational data store) richer information, history, etc.
    c. UMBC: Bio/demo changes in PS, PS processes put unique ID in a table that indicates there was a change, IAM scans that table, grabs the whole current record and filters for changes.

5. Next steps?
    a. BenR ISU: Diagram / Spreadsheet summary of current practice, plans; e.g. Tommy's concept of roles is widely different than ISU; pre–hires entered as 'guest' security role. Switch from OIM to Grouper in future, and then back to PS;
    b. JeffC: PS to manage access (dept. Org, don't use job code; Reconciliation to true up after messaging failures. Tough to get the right granularity of user info to the campuses; granting services to pre-hires, what is the policy def of pre-hire. HR PS

Decisions and Action Items

- Potential new work item: Create something (diagram, spreadsheet,...) that allows for comparisons across campuses in how PS and IAM are integrated.

Friday, February 25, 2022, 10:00 am Eastern, 7 am Pacific, 3 pm London

Participants

1. Tommy Doan - SMU
2. Pery Doan - SMU
3. Keith Hazelton - Internet2
4. Andrew Parmer - University of Florida
5. Ethan Kromhout - UNC Chapel Hill
6. Robert Rust - UW-River Falls
7. David Bickel - Indiana University
8. Jeffrey Crawford - UCLA
9. Benjamin Rappleyea - Illinois State University
10. Jeremiah Haywood - Illinois State University
11. Carmen Plummer - Illinois State University

Agenda

We may not cover all of this in one meeting, and that's fine. The intent here is to mark a path for the working group. Comments and recommendations are always welcome!

6. PeopleSoft and IAM integration recommendations
    a. Objective: Develop a reference document for PeopleSoft developers for one or more common interfaces that will work with each IAM software component.
    b. Below I'm thinking about identity synchronization strategies. In future calls we'll discuss Grouper strategies, and also explore midPoint provisioning thoughts.

    c. What data elements should be shared between PeopleSoft and IAM?

        i. NOTE: This working group has discussed whether to provide University affiliation as something calculated within PeopleSoft. Perhaps it's no surprise, but it seems each campus has its own unique perspective on this. Let's pursue other types of data.
        ii. JeffreyC; System-level HCM: (only for non-students) Names, date of birth, employee number; SSN used for match, then discardedDepartmental info, campus location, highest % appointment becomes primary; Looking at IGA, right now a staging db and an LDAP behind an API,
        iii. PeryD; SSN? JeffreyC: When something happens on PS, we get a SOA message including an encrypted SSN; If match linked and SSN discarded, If unclear, put in a resolution workflow. Once it's handed off, SSN info is excluded from the DB
        iv. DavidB, IU: Sync process between PS Student & HR; plan to move to a COmanage registry. Search-Match plus cleanup of duplicates; PS is only SoR, other affiliates are entered into PS; COmanage will shift affiliate handling; COmanage intended to resolve duplicates; Data elements: Partial SSN under debate, DoB; Tel. number and type (office,

emerg), emails and types (voluntary, self-asserted (stand-alone, moving to COmanage); Will leverage COmanage for affiliates, continue to use PS S/M

v. Ethan: Syncing identities use PS S/M, and PS is the primary registry; migrating to midPoint at some point; person and demo data. Not ssn, dob, bring over dept. Year, etc; HCR: Jobs, associations from Campus Solutions; Coming from Health Care system will get a record created in PS; COmanage planned for researchers, so outside PS; Acceptable to carry duplicates across PS and COmanage, eventually perhaps COmanage ID Match; Course info into grouper

vi. RobertR, UW RiverFalls; 1 way flow into MS identity manager, directory information; class enrollments to build AD groups for course rosters, as needed, not all classes; For classes needing software; All identities come in through PS; Interest in Grouper, perhaps midPoint; Long-term Affiliates brought into PS as employees, short-term affiliates, create a temporary, expiration-dated ID.

vii. TommyD, SMU; COmanage as registry, PS as primary SoR but other systems will be there; Name, DoB, email and mobile number;

viii. What data do you provide **from PeopleSoft to IAM**? What data do you provide **from IAM to PeopleSoft**?Which are required and optional?

1. How set up how decided
2. Ethan: CS into messages into IAM system; based on triggers, any change that IAM cares about sparks a message; HCR has 2 Home-grown…IAM-side web services: 1) incremental (every 10'); 2) Full reconciliation once a week.
3. BenR: messaging, but OIM can be overwhelmed at major turnovers; Moving to a view/table with a lastModified column they that mP will bring in via live-sync; Full reconcilitation under consideration
4. When do you trigger changes, there's the basic identity info and there's the affiliation/role data; BenR: at point id is created or modified: Ethan CS: If a user is created or altered in any way; If an affiliation changes, student record; When new person gets provisioned to target; Ethan: record would flow even w/o affiliation, marked 'private' and LDAP created; ISU: Empl created by PS in CS; Created in PS roles, and that's transmitted; CS come in via Slate, only when they reach afl-prospect, assigned enrollment data, moves to student: ugrad, grad, continuing ed; dynamic roles in PS prospect, admitted, Eventually Grouper will handle and pass back to PS; SCG suggested holding off creation of registry record until there's an assigned job or admitted student; only then into CS and IAM system; Admitted get central systems identity and services; 3rd party email address from Slate to PS to IAM; Slate does ID match for students; PS passes an id back to Slate (University Login ID, and EMPLID); Slate is SaaS where applicants; UNC, Slate produces a CSV file that's transformed into PS processable format and imported into CS; UWRF, UCLA also use Slate; DavidB, Indiana U: homegrown w PS, looking at COmanage as replacement;
5. TommyD: Similarity across handling of identity data, not so much the case for affiliations; Data elements other than basic identity data and affiliations? Continue in next call: What data do you provide **from IAM to PeopleSoft**? (see item ix) below

6. Possible objectives. Are there others?

a. Person registry functionality
    i. Provide directory information that allow systems and people to distinguish users who have common attributes, e.g. John Smith.
    ii. Facilitate identity matching with identities sourced from other systems.
b. Access control management

ix. What data do you provide **from IAM to PeopleSoft**? Which are required and optional?
1. Possible objectives. Are there others?
    a. Create an immutable link between identities in PeopleSoft and IAM.

d. What technology do you use to export the data for a one-time data conversion export?

e. What technology do you use for ongoing synchronization?

f. What triggers the synchronization?

Decisions and Action Items

Friday, February 11, 2022, 10:00 am Eastern, 7 am Pacific, 3 pm London

Participants

1. Tommy Doan - SMU
2. Keith Hazelton - Internet2
3. Todd Haddaway - UMBC
4. Andrew Parmer - University of Florida
5. Ned Morgan - UNC Charlotte
6. Jeremiah Haywood - Illinois State University
7. Benjamin Rappleyea - Illinois State University
8. Ethan Kromhout - UNC Chapel Hill
9. Pery Doan - SMU
10. David Bickel - Indiana
11. Geethani Cabraal - Illinois State University
12. Jeffrey Crawford - UCLA

Agenda

1. Peoplesoft data, IAM components and the concept of affiliations.
    a. What do we mean by affiliation?
        i. Coarse-grained
            1. Values from eduPersonAffiliation: student, faculty, staff, affiliate…Computed at the System of Record (like PeopleSoft); Registry carries basic bio-demo data plus the coarse-grained, high-level affiliations
        ii. Fine-grained:
            1. Tend to be campus specific; differentiate from coarse grained; where and how the values of these attributes
        iii. Challenges with the notion of “primary” value; Started with coarse grained queries against PS, passed to OIM; Finer affiliations turned out to be more important. 30 queries now against PS, pass along to OIM as finer-grained affiliations. Primary affiliations computed in OIM
        iv. UNCC: Pull data based on a loosely affiliated definition in part to limit identities that need to be pulled into the IdM system. Actual affiliations, faculty, staff, student, defined in IdM; Anything finer grained calculated in the IdM system. Currently focused on refining types of employees.
        v. Illinois State U also using midPoint
        vi. SMU moving away from PS as their person registry; Need a registry solution not based on ERPs. Using COmanage in that role. ID Match will be used to unify individuals across systems of record.

vii. ToddH: Looking at COmanage for guests, so it will become a source system into the official person registry
viii. SMU: Once registered in COmanage, person is issued a NetID as well as an enterprise ID, both sent back to PS. So transition from guest to student will be smooth
ix. UCLA: PS for employee side, so IAM done at campuses (with Grouper or existing IdM system); Person Registry is fed from central HR to each campus. The campuses manage the affiliations, coarse and fine-grained. No barrier to a campus adding people into PS. Information flows both central PS to campuses and campuses to central PS
x. BenR: information does flow both ways at Illinois State University, ERP to midPoint and midPoint to ERP

b. Why do we need affiliations?
    i. Access management
    ii. Service eligibility
    iii. Are there additional purposes for assigning affiliations?;
        1. Policy enforcement
    iv. JeffreyC: NIH is an example of a global service. Entitlements (local) vs fine-grained affiliations (more global);
    v. Provisioning: Home grown with increasing use of Grouper. Now there is Interest in an Identity Governance and Administration (IGA) tool, so Grouper migration is on hold.
    vi. UNCC have a mix of fine and coarse grained affiliations that factor into determining the password reset policy (e.g. students get a longer password lifetime); OpenIdM manages the policy; Extended period if you're in Duo as well. Sys admins have to change their passwords every 90 days. OpenIDM similar to midPoint. But OpenIDM not as performant as the combination of midPoint and Grouper. OpenIDM at about its functional limit. Dismantling and reassigning out to Grouper and/or midPoint.
    vii. ISU: Provisioning, Microsoft Office Licensing, web portal view customization

c. What level of affiliation should be determined by PeopleSoft versus IAM systems?
    i. (See 1.a. above)

d. How are campuses currently calculating affiliation with PeopleSoft? What enhancements are planned?
    i. We may all benefit from multiple presentations here.
    ii. Ideally we can arrange a schedule of presentations and or informal discussions with participating campuses

e. How can that affiliation data be presented to IAM systems?
    i. In scope for this working group. Affiliation is likely to be a category of information that needs to be presented out to IAM systems

Decisions and Action Items

Friday, January 28, 10:00 am Eastern, 7 am Pacific, 3 pm London

Participants

1. Tommy Doan - SMU
2. Majeed Abu-Qulbain - Illinois State University
3. Ben Rappleyea - Illinois State University
4. Jeremiah Haywood - Illinois State University
5. Anderson Klay - Illinois State University
6. Keith Hazelton - Internet2
7. Jeffrey C - UCLA
8. Todd Haddaway - UMBC
9. Robert Rust - University of Wisconsin-River Falls
10. Andrew Parmer - University of Florida
11. Ethan Kromhout - UNC Chapel Hill
12. Bill Kaufman - Internet2
13. David Bickel - Indiana University
14. Pery Doan - SMU
15. Richard Frovarp - NDSU
16. Thomas Carter

Agenda

1. Any suggestions or revisions to the Working Group Charter to help us come up with practical, useful information for people?

2. Illinois State University's official definitions of affiliations/roles from PeopleSoft data (Majeed Abu-Qulbain, Ben Rappleyea)

    a. ISU Identity Data Dictionary: https://docs.illinoisstate.edu/identity/topics/affiliations
    b. Majeed, Ben, Jeremiah (Anderson Klay maintains the data, Dan, CISO sponsored)
    c. 2014: Campus Solutions, HCM already there; affiliations were a gap, definitional chaos
    d. Confluent templates and page structures, InfoSec
    e. IAM reports to CISO Dan Taube; Majeed is Architect, Ben, Jeremiah Office of IdM
    f. Primary affiliation got used as tool for managing licenses
    g. ToddH: Who uses this? Different stakeholders need different subsets of attributes
    h. Mass mailing people; people who want a group sent here; Sysadmins bringing up new services that they want to control access to
    i. Majeed: Request for managing access to ? learning app; Collaborative definitions of the data elements

j. Todd: Helpful to clarify misunderstandings of meaning
k. Tommy: Official reference is useful; What process to define all these?
l. Ben: Project took about a year; initially to clean up AD & LDAP groups, brought together HR, Students, Applications; Clarified and tweaked the definitions. Gradually grew from 15 to near 30. Partners defined the priorities, IAM took back seat
m. “Instructor” covered a broader set of folks than have official definition of instructor
n. Adjunct? Broadly defined, expanded recently; HR codes them and defines the query
o. Used enrollment date to move prospect/applicant to ‘student’; at end of term, transition to ‘grace’ for a year, maintain access to email, campus login
p. Do you have a companion doc to define the student / employee lifecycles. It’s not a public document per se
q. TommyD: Seems valuable to explicitly define and publish these lifecycles
r. Directory info, groups, provisioning
s. Majeed: Today driving permissioning off base affiliations
t. Fine tuning, e.g. email provisioned closer to the actual enrollment date

3. To provide info from ERP to IAM system: Major requirement is to expose affiliations and figuring out how these are derived from PS data. Where is that biz logic applied
    a. Majeed: Dynamic roles: PS queries based off internal dynamic roles; Opted not to use PS built in affiliation functionality; Moved to version controlled environment; PS query populate Dynamic roles for internal; These queries will be moved into Grouper to maintain a centralized; Complement these definitions with the queries that populate them;
    b. Authenticated version does have that in the staff viewable version of these definitions; change management for the queries themselves, IAM and HR reviewed
4. Feedback, questions from PS devs on the call?
    a. Similarities to other institutions
    b. Smart use of dynamic roles in PS; how will Grouper recreate those data elements? Still discussing how those get back to PS; Async? ISU-specific table?
    c. PeryD: We use the PS-provided affiliation framework table;
    d. Use of PS Affil tools; Developer worked in dev environment and his affiliation data got overwritten on move to the production; PS to OIM complexities as well;
    e. PeryD: Sponsored accounts moving out of PS, how do you maintain visibility; We are pushing back into PS, where they get an EMPLID;
    f. Slate framework for getting identities into PS via batch (PS constituent framework)
    g. Majeed: Moving identity creation from OIM to PS, Before, creation flow was bi-directional SEC coincident sync got info from OIM to PS. Creating multiple EMPLIDs, loops between OIM and PS; User profile create and update messages sent from IAM to PS. Idempotent behavior has been very reliable, no duplicates. Will continue to use going forward. Will push email address back to PS, send over the consent message to PS, affiliation data will flow

5. Volunteers to share their stories in two weeks?

Decisions and Action Items

Friday, January 14, 10:00 am Eastern, 7 am Pacific, 3 pm London

Participants

1. Tommy Doan - SMU
2. Pery Doan - SMU
3. Robert Rust - UW River Falls
4. Geethani Gunasena - Illinois State University
5. Ethan Kromhout - UNC Chapel Hill
6. Todd Haddaway - UMBC
7. Carmen Plummer - Illinois State University
8. Andrew Parmer - University of Florida
9. Eric Crossman - University of Florida
10. Keith Hazelton - Internet2
11. Andrew Thompson - Illinois State University
12. Jeremiah Haywood - Illinois State University
13. Benjamin Rappleyea - Illinois State University
14. Majeed Abu-Qulbain - Illinois State University
15. Nathan Stien - Illinois State University
16. David Bickel - Indiana
17. Joanne Boomer - University of Missouri
18. Bill Kaufman - Internet2
19. Anderson Klay - Illinois State University
20. Richard Frovarp - NDSU

Agenda

Around the room; Please share the following: Bring PS developers as possible

a. Name and institution
b. The type and role of Peoplesoft ERPs currently in use and/or in planning at your institution
c. Beyond students, faculty, and staff, what types of university affiliations does your PS system include
d. What connections exist between PS systems and other campus systems
e. What are the technical foundations of integration between PS and other systems
f. Are there projects in planning or in progress that will lead to changes in your answers to the above?
g. Any other noteworthy features of your ERP and IAM infrastructure

2. TommyD: **SMU** IAM Team, PS since 2000; CS, HCM, Financials; 12k students, 3500 employees (all in PS and PS is their Enterprise Person Identity Registry; CS bolt-on since 2010 to handle access management, provisioning

3. RobertR, Integration Engineer, **UWRivFall**, 5,000 students 1,000 employees CS,; UW System hosts HC for the campus. Handful of AD accounts, but most people are in PS; interface with Microsoft identity manager; Hoping to move to midPoint at some point. Prov targets, MS IdMgr, Canvas, Rec sports,..ID Card gets a flat file plus MSIM integration;
4. **Illinois State U**, BenR, Geethani (PS dev), Carmen (PS dev) Nathan (Integrations Developer), Andrew Thompson (Integrations Developer), Jeremiah (IAM), Anderson (IAM), Majeed (Enterprise Arch),: CS, HCM (2011-13) OIM, 21K ugrad, 3K grad, 4K staff; moving off OIM to mP, Grouper; Majeed: messaging from CS to OIM was cumbersome, so didn't use affiliation framework or dynamic roles; instead used PS queries to determine roles, Nathan Stein: AndrewT: aff framework was tricky. Pery Doan, SMU, interested in affiliation manager for population definition/selection. Majeed: PS integr sends affil messages, OIM has a message listener; but moving to mP live sync via triggers to Db identity table; PS dev: PS batch job generates table, specific triggers (create, etc) message to OIM plus messages update the identity table; that drives mP live sync. Inbound PS to mP, to Grouper via loader jobs. TommyD; ISU_DENTITY App Engine runs everyday at 11AM (It makes sense that we decide to run it only once a day since we also have the event based triggers also updating the table upon various types of "save" events); Diagrams would be super helpful.
5. Ethan, **UNC Chapel Hill**, 70K in IdM;; PS HCM, Finance, CS; CS is person registry, everyone gets Emplid; 15 affiliations outside fac/staff/student bring them in; PS Integration Broker to IdM; Integration wi HCM and Finance via APIs(?); Moving to mP for Registry in order to manage non-person entities. Person Basic Sync between PS modules, but outbound to other systems
6. Todd H, Director for IAM **UMBC** 15k students, 4k fac/staff; CS, HCM on prep, Finance is in AWS; PS is registry for all populations, sent to era 2000 custom IAM; PS to Grouper; messaging from CS to IdM (new ppl, changes); APIs, messaging, Informatica emerging as integrated data hub. Salesforce (recruiting) and data warehouse get PS data from Informatica; Containerized Web Servers, 12 prod servers, patch ahead of time, role into prod. 1 gotcha: HCM still has some MS Cobol license; that license doesn't play nicely in containerized env: demands a special containerized Cobol. Not using affiliation framework; Affiliations derived/assigned in the homegrown IAM systems (2001 era Perl); Moran evaluating IAM system, but probably won't go commercial.
7. Andrew Parmer: **UF**:60k students, 15-20k employees, HCM, CS, FI, IBM MDM for identity; custom role request on top of PS; PS manages lifecycle for modal identities; Future: Access request moving to Grouper (in prod) and midPoint; Account mgmt move from PS to mP. PS pushes affiliation data to MDM (not using affiliation framework), looking to leverage Grouper for affiliation management rather than MDM. Eric Crossman: CSP participant this year; Looking at COmanage registry for guests (and perhaps others down the line);
8. David, **Indiana U**, Sys engr. Emp, students, friends; 50k employees, 150k active students; Total identities 500k; simple feed file dump 4 times daily to MS IM; bringing PS data into mP; Hopefully moving to an API ve flat file approach;
9. JoanneB (IAM team mgr), **U Missouri System**: 4 campuses + hospital; 1 HCM (2001) 1 FI, 4 CS 2000s; 70k students, 30k employees; HCM has 2 companies; main plus RET (retirement system) person can be in both companies, 'courtesy appointments' in HR for longer-term visitors except for Hospital which has different rules for who can have a courtesy appt; EMPLID is synced across PS systems using search/match functionality; Feeds from PS, use PowerCenter (ETL), transforms data for IAM and other downstreams; Homegrown IAM systems, hourly feed ot changes plus a full update; Implementing Grouper about to create data feeds from IAM to Grouper;
10. RichardF **NDSU**; 12k/3-4k; System runs PS for his campus; SOAP requests to run queries that feed Grouper and midPoint; Photos and billing records pushed TO PS

11. With reference to the Working Group Charter, what kinds of products from this group might provide meaningful assistance to institutions adopting or evolving their PS infrastructure?
    a. Homework: Review charter and we'll discuss again at our next meeting on Jan 28.
    b. ToddH: One useful deliverable would be a document about PS to Grouper integration: 'Here are common PS queries that provide useful information to Grouper when building loader jobs:
    c. MajeedA ISU hss published definitions of affiliations/roles, those are used to build loader jobs;

Decisions and Action Items

1. [All] Review charter and discuss at our next meeting on Jan 28
2. [Internet2 IAM] Information about PS there.