Kuali Rice IdM Notes

Draft

This document is currently being drafted, the below should not be considered complete by any stretch of the imagination

Content

Background

Over the past few weeks, we briefly met with various Rice Application and Institutional stakeholders along with a pair of Commercial Affiliates to get their input on what the essential functions of a full IdM application should be. Below is a summary of the most important and common pieces of feedback that we received. Additionally we've provided some use case examples for some of those pieces.

Major Pieces

Identity Data Management

- Person Registration and Profile Management
  - Relationships to Persons
  - Life Long ID
  - Non-Person registration (vendors)
  - System Profiles
- Identity Reconciliation ("Identity Match")
  - Duplicate/Matching Logic
  - Merge Duplicates
- Compliance and Privacy
- Identifier Management
- Authenticator Management
- Group Management
- Role Management
  - Make sure that extends to Application security
- Access/Permission/Privilege Management

- Attribute Management
- Identity Data Workflow
- Delegated Administration and Self Service
- Federation of Identity Data
    - PESC Data Standards
- Modern UI
- Up-to-date Documentation

Identity Services

- Provisioning and De-provisioning
    - Onboarding and Continuous Auditing
- Authentication
- Authorization
- Directory
    - Person Registry
- Single Sign On (Local and Federated)
- Connectibility
    - Existing ERPs
    - Address Services
    - Access to external data stores
- Batch Processing/Syncing
- Presence and Location
    - Distributed Sessions
- Reporting
    - Access Certification

Application Requirements Boxing

Person	Management	Workflow	Security	Tools & Integration
Person Registration and Profile Management	Identifier Management	Identity Data Workflow	Authentication	Connectibility
Identity Reconciliation	Authenticator Management		Authorization	Batch Process/Syncing
Compliance and Privacy	Group Management		Directory	Reporting
Delegated Administration and Self-Service	Role Management		Single Sign On (Local and Federated	Modern UI
	Access/Permission/Privilege Management		Presence and Location	Up-to-date Documentation
	Attribute Management		Federation of Identity Data	
	Provision and De-Provisioning			

Use Cases/User Stories

Kuali Student: Provisioning

Description: A student signs up (and is accepted) into a class, the should automatically have access to class specific areas (wiki's, syllabus, class chat area, research documentation, etc.)
User(s): Students, Faculty
Business Owner(s): Registrar, Faculty
IdM Opportunity: Seamless provisioning solutions that automatically grant access specific to needs based on entitlements a user has streamlines their ability to immediately get the information they need. It also allows for those that need to disseminate the information, to worry less about how it gets out and if it gets out and to focus on the content instead.

Kuali Student: Duplicate/Matching Logic

Description: Often times there are multiple users entering new students into a system, this can lead to the creation of duplicate system ids for a single person. Registrar accreditation is dependent on this. i.e. Student leaves and comes back later, making sure that the record is maintained over time (can't just make a new person each time).
User(s):
Business Owner(s):
IdM Opportunity: Create an IdM service that allows application areas to specify the attributes that are checked when adding a new person to determine potential duplicates.

Kuali Student: Federated Identity Data

Description: Students who are taking courses at multiple schools, setup easily and cleanly across those schools systems. Still provide local control, not quite batch syncing, but more seamless. Includes faculty that instruct across different universities/schools; persons that are interacting with multiple institutions at the same time.
User(s): Faculty, Staff, Students
Business Owner(s): Institutional IdM administrators
IdM Opportunity: A federated identity structure would allow more institutions to interact with each other more efficiently when faculty, students, and staff are engaged in activities with multiple campuses or institutions. With the data federated, parts of the person data, their roles and groups wouldn't necessarily have to exist in both systems, the receiving system could honor/use those from the sending system. Done right, this type of interaction could lead to a more widely adopted and richer system.

Kuali Student: Merging Duplicates

Description: Even with complex matching logic, there are still cases where a single person may be added into a system with multiple ids. Having a single id is essential to keeping a clean and complete record of a person.
User(s):
Business Owner(s):
IdM Opportunity: An IdM service that would provide a quick and seamless tool for merging multiple records into one would allow for cleaner data and a complete record of a person for current and historical purposes.

Kuali Student: Relationships to Person

Description: Parents of students, immigration (family or extended family). For granting proxy access to records; some level of access.
User(s): Parents, Faculty, Students, Former Students, Alumni, Guardians
Business Owner(s):
IdM Opportunity: Backed by Role Management, a person could identify the role of another person thereby giving them proxy or access to select pieces of their information.

Kuali Student: Role Management

Description: Former students or alumni still need access to their student records at an institution even if they are not currently enrolled.
User(s):
Business Owner(s):
IdM Opportunity: A robust Role Management infrastructure would allow for permissions and access to be limited based on the role (Alumni, Former Student, etc.) of the accessing person.

Kuali Student: Distributed Sessions

Description: Changes to a piece of data, if you're in an application to request transcriptions, receive a financial warning block, click on a link, passing where the user came from and what their context is. Sharing that information across applications. Monitoring timeouts for stale sessions.
User(s):
Business Owner(s):
IdM Opportunity: Presence, Location, and Authorization pieces of an IdM system should work together to recognize when person is operating in multiple sessions across applications and react appropriately (adjusting time outs, etc.) when this is happening.

Kuali HR: Connectibility

Description: Address and their accuracy over time is critical to an institutions ability to effectively maintain in contact with faculty, students, employees over time.
User(s):
Business Owner(s):
IdM Opportunity: External vendors provide plug-in options for validating address information in real time during entry that many institutions have found to be extremely effective in collecting clean/correct addresses. While the creation of a service within would be optimal, at a minimum an IdM could provide easy ways for institutions to continue with these plug-in options.

Kuali HR: Provisioning and De-provisioning

Description: As people are hired or change positions, many times it leads to delays and requires multiple contacts/requests be made to ensure they have the correct access. Additionally, when they leave, the removal of access is often a catch up process.
User(s):
Business Owner(s):
IdM Opportunity: Provisioning and De-Provisioning tools and logic with configurable notifications or workflow associated with these processes would ensure that employees are quickly "onboard" or removed from access setups where necessary when they move or leave.

Kuali HR: Role Management

Description: When and employee is terminated, you need still provide long term access to Tax data w/out giving them full access based on their prior roles.
User(s):
Business Owner(s):
IdM Opportunity: Having effective and easy to configure Role Management tools will allow institutions to grant limited access to these (sometimes) large groups of former employees as federally required.

Kuali HR: Life Long ID and Person Registry

Description: Alumni and Retirees (Endowment), work w/CRM. Keeping a single ID for person over the life cycle of the person.
User(s): Faculty, Staff, Alumni, Retirees
Business Owner(s):
IdM Opportunity: A single, institutional source to store all persons, with a single ID that remains with the person for all phases of their interaction with the institution allows for clean, long term, historical data while reducing the potential for a single person having duplicate IDs. With out this, a person may exist in multiple systems and thus result in a fragmented and incomplete representation of the person in all.

Kuali HR: Batch Processing/Syncing

Description: Fewer sources of data, with better security around it, the better off and cleaner the data will be and easier to keep up-to-date.
User(s):
Business Owner(s):
IdM Opportunity: The aim of a single person registry would negate the need for batch process, there will still be instances where person records need to be sourced or synced from areas outside the IdM. Providing and infrastructure that makes this as easy and quick to setup as possible will allow for easier adoption.

VivanTech: Modern UI / Reporting

Description: A support desk needs to easily be able to see what access and permissions a person has and why they may not be able to perform a task they need to.
User(s): Support Desk Personnel
Business Owner(s):
IdM Opportunity: An IdM application with usable tools for end users to easily audit and trouble shoot access issues and needs.

Kuali Financial System: Profiling

Description: In an institutional framework where many of the applications are Kuali based, users need to be able to go to a central location to review or update profile options that maybe be shared across the applications. KFS and Coeus has a situation right now where the sets are the same but need to be specified and maintained in each. Related to travel, chart/account info, user preferences etc. are stored in a profile. User preferences are being spread across multiple platforms/applications.
User(s):
Business Owner(s):
IdM Opportunity: Service where users can audit this information in a central place instead of going to multiple spots. Having a central profile and being able to audit it (by user or by administrator) would provide value by not having to build profile sets out in multiple systems.

rSmart (Boston College): Compliance and Privacy

Description: Students need to be able to exercise their FERPA right to suppress some home directory information. Staff that have a business need should still be able to see all the student's data including those suppressed items.
User(s): Students
Business Owner(s):
IdM Opportunity: A flexible utility for defining and enforcing compliance and privacy regulations will allow for easier localization of an IdM solution at a wider range of institutions.

rSmart (Boston College): Relationships to Persons/Role Management/Provisioning

Description: A user is and employee and an Alumni. Their child enrolls, so they become a parent. With no termination or change to existing access/service /etc., they are now given access to parent transactions in the portal and/or any other parent access right.
User(s):
Business Owner(s):
IdM Opportunity: Having a cohesive set of tools that work together automatically will reduce the burdens of setup and adoption as well as providing more real-time identification of what a person should have.

IU: Access Certification

Description: An auditor of IT should be able to sit down without any explanation and independently audit the access control.
User(s):
Business Owner(s):
IdM Opportunity: Open source does Access Policy Management OK, and Access Certification badly. Good Access Certification does risk points, if you get over a particular risk, you are then ranked as being a risk because of what you can do; risk based targeting. Having a rich Access Certification would give an IdM a tool that provides value and security for adopting institutions that most open source solutions do not offer.

Kuali Coeus: Federation of Identity Data

Description: In the research area relates to multiple identities across multiple areas (NSF, NIH, Contractor Registry, etc.) All have their own passwords and roles, the federation and playing nicely between these are critical and not handled well. NIH has a series of 7 level 3 bio-containment labs across the US , and each lab has it's own identity management process based on the individual institutions. They've had to create a separate IdM solution just for this case, a separate LDAP directory was created that has to be managed (passwords, maintenance, etc.)
User(s): Researcher, faculty, students
Business Owner(s):
IdM Opportunity: Having common, federated standards will allow for more efficient and seamless role identification between various applications, systems, government agencies, and institutions. Collaboration is better.

Iowa State: Role Management

Description: A student graduates and becomes an employee. This employee later takes a class becoming a part-time student again. Later, the employee may be the parent of a student. The employee has all of these roles in parallel: alumnus, employee, student, and parent.
User(s): Students, Faculty, Staff, Parents, Vendors, etc.
Business Owner(s): Registrar, HR, Alumni organization, Admissions, etc.
IdM Opportunity: Defining a person once and assigning multiple roles is much less error-prone than defining separate "persons" for each of their roles. Assigning access and entitlements will need to take all roles into account.

Iowa State: Batch Processing/Syncing

Description: The Facilities department assigns keys and proximity card access based on employment status. The key system is separate from central administration and relies on a data feed for status updates.
User(s): Faculty, Staff, Graduate Students, Student Employees
Business Owner(s): HR, Facilities
IdM Opportunity: Information required for "external" system updates is expected immediately. A batch process may not be timely enough and may even be a security risk. Standard real-time interfaces and queries to IdM data may be required with proper authorization.

Kuali OLE: Provisioning and De-provisioning students

Description: A student registers for the semester or quarter, they should automatically have library privileges, to enter building, use library workstations, circulate books, recall books, other services, also access electronic resources licensed by the library. When they are no longer registered, privileges change. Privileges may vary based on geographic location (e. g. e-resources licensed for access to Chicago campus, not Beijing or London).
User(s): Students
Business Owner(s): Registrar
IdM Opportunity: Seamless provisioning solutions that automatically grant access specific to needs based on entitlements a user has streamlines their ability to immediately get the information they need. It also allows for those that need to disseminate the information, to worry less about how it gets out and if it gets out and to focus on the content instead.

Kuali OLE: Provisioning and De-provisioning non-university, non-federated users

Description: As library adds non-university researchers, they should automatically have certain library privileges, to enter building, use library workstations, circulate books, recall books, other services, also access electronic resources licensed by the library. Privileges vary with type, may be visiting researchers in Special Collections, special libraries that purchase access to certain resources, general public accessing a Federal Documents Depository. When they are no longer registered privileges change.
User(s): external borrowers, readers
Business Owner(s): Library
IdM Opportunity: Provisioning and De-Provisioning tools and logic with configurable notifications or workflow associated with these processes would ensure that employees are quickly "onboard" or removed from access setups where necessary when they move or leave.

Kuali OLE: Federated Identity Data

Description: Students who are taking courses at multiple schools, should be setup easily and cleanly across those schools systems. Still provide local control, not quite batch syncing, but more seamless. Includes faculty that instruct across different universities/schools; persons that are interacting with multiple institutions at the same time. Consortia of libraries may use a single OLE system and need to add students/faculty/staff from multiple institutions. A group of libraries may have a Reciprocal Borrowing agreement, although they have separate library systems (OLE or other). Library privileges may vary by agreement. Hathi Trust will offer access to copyright restricted materials for disabled students.
User(s): Faculty, Staff, Students
Business Owner(s): Institutional IdM administrators
IdM Opportunity: A federated identity structure would allow more institutions to interact with each other more efficiently when faculty, students, and staff are engaged in activities with multiple campuses or institutions. With the data federated, parts of the person data, their roles and groups wouldn't necessarily have to exist in both systems, the receiving system could honor/use those from the sending system. Done right, this type of interaction could lead to a more widely adopted and richer system.

Kuali OLE: Relationships to Person

Description: For granting proxy access to library privileges. It is common for a faculty member to assign his/her library privileges to a graduate student helping them with research
User(s): Faculty
Business Owner(s): Library?
IdM Opportunity: Backed by Role Management, a person could identify the role of another person thereby giving them proxy or access to select pieces of their information and to their library privileges.

Kuali OLE: Role Management

Description: Former students or alumni may have more limited library privileges. E-resource licenses usually do not include them. Borrowing privileges expire although they may continue to enter the building and use resources on site. They may purchase additional borrowing privileges from the library. Even when privileges expire library retains records for items still checked out and fines still owed. When an employee is terminated their library privileges end. Library retains records for items still checked out and fines still owed. A student who works at library, when they stop working need to have permissions to update/edit records removed. Grace periods may vary. Email and e-resource for student stay for 6 months. Library borrowing privileges expire immediately on graduation. Need Expiration date for library borrow privileges. Also if Library fees are not paid and materials returned, often students are not allowed to graduate or register for classes. Ability to share this restriction with Registrar system would be useful.
User(s): Alumni and former students; Former employees
Business Owner(s): Library
IdM Opportunity: A robust Role Management infrastructure would allow for permissions and access to be limited based on the role (Alumni, Former Student, etc.) of the accessing person.

University of Arizona: Connectibility

Description: Need to be able to implement attribute based access control with defined polices in a central area used to provision roles, but allow the institution to use pieces that are already in place and leverage the IdM suite pieces needed
User(s):
Business Owner(s):
IdM Opportunity: The IdM suite has to be flexible enough to allow an institution to leverage/use the pieces of the suite they need while working with IdM solutions they may already have in place in a seamless fashion.

Summary Slides

A slide deck which includes a summary of findings:

- KualiIDMSummary.pptx
- KualiIDMSummary.pdf