Registry Subcommittee Deliverables

Group Name:

Identity Registries

Date:

8/12/2011

Purpose of Group:

Come up with plan to move forward of the current gaps in identity registries, aka person registries; looking at options for developing single registry that could be open and used by various institutions/organizations. moving forward to close the gaps by developing a registry

Model, Scope, and Glossary

There is a Identity Registry Functional Model which describes scope and functions and terminology of the Registries "chunk" in narrative form.

The original scope listing is:

1. matching
2. id store: schema, interfaces, object
    a. persistent storage of identity
    b. multiple credential
    c. multiple identifiers
    d. multiple affiliations (types of relationships) with the organization
3. registrations
4. management functions
5. notification
6. reconciliation
7. identity merge
8. life cycle/statefulness

This Glossary provides an alternative definition of terms:

Term	Definition
Affiliation	Affiliation is the combination of one's relationship with an institution (which may allow access to electronic services) and some form of *trusted* (may not be University) identity.
Assurance Levels	Assurance levels are numerical levels (or degree levels) that correspond to the degree of confidence in the vetting and proofing processes used to establish the identity of the individual to whom the credential is issued (Levels of Assurance)
Attribute	Information associated with a digital identity record. Attributes may be general or personal. A subset of all attributes defines a unique individual. Examples include name, phone number, and group affiliation.
LoA	The degree of confidence in the vetting and proofing processes used to establish the identity of the individual to whom the credential is issued. Levels of Assurance also consider the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued.
Vetting	The process of validating information, collected from an individual, for the purpose of issuing digital credentials.
Credentialing	The act of issuing a token that will be used to establish a digital identity.
Proofing	The act of aligning a person's previously recorded data to the actual person at the time when credentials are issued. In-person proofing involves checking a photo ID, such as a driver's license, against the holder of the ID.
Affiliate	A person who has some connection to the University.
Net Id	An electronic identifier created specifically for use with on-line applications.
Identity Assurance Profile	A set of data, associated with an individual, that relfects the degree of confidence in the vetting and proofing processes used to establish the identity of the individual to whom the credential is issued at a given point in time. See "Assurance Levels" and "lLevels of Assurance" for related information.

Requirements/Principles of the Chunk/Module:

✅ = Fit, ❌ = Gap, ⚠️ = Roadmap Item

Identity Merge

Despite the best of tools to identify and prevent the entry of duplicate identities into an Identity Registry, duplicate identities will inevitably be created. The Identity Merge facility will provide the ability to link or merge identity data to a single unique identifier.

Requirement ID	Requirement Source	Requirement Description	KIM	PSU	Open Registry
REG_0001	A. Neal	The Identity Merge facility shall provide the ability to link unique identity records within the registry identifying one as the primary.	⚠	✓	✓
REG_0002	A. Neal	The Identity Merge facility shall maintain for historical purposes the non-primary registry entries. These entries shall not be available for further use (other than historical reporting) in subscribing systems.	⚠	⚠	✓
REG_0003	A. Neal	The Identity Merge facility shall provide the ability to merge identity data to a "primary" registry entry through either an automated process or a user controlled process (eg. system identifies records to merge, shows user relevant data, user decides interactively what to accept etc.)	⚠	✓	✓
REG_0004	A. Neal	The Identity Merge facility shall provide notifications to subscribing systems of the merged identities	⚠	✓	⚠
REG_0005	A. Neal	The Identity Merge facility shall provide for the creation of business rules for the automated merging of registry data elements. (eg. defining the authoritative source by attribute when duplicates are identified)	⚠	✓⚠	✓⚠
REG_0006	A. Neal	The Identity Merge facility shall be integrated with the Access Management Module to allow for assessing and potentially merging role and access data when duplicate identities are identified and merged.	⚠	⚠	⚠
REG_0007	A. Neal	The Identity Merge facility shall be integrated with the Provisioning Module to allow for the potential deactivation of duplicate accounts.	⚠	⚠	⚠
REG_0008	PSU	The Identity Merge facility shall use a fuzzy logic searching capability for matching purposes.	⚠	✓	✓⚠

Registry

The registry is the core data store of identity information. What follows are requirements related to it.

Requirement ID	Requirement Source	Requirement Description	KIM	PSU	Open Registry
REG_0100	PSU	The registry shall support the storage of identity information.	✓	✓	✓
REG_0110	PSU	The registry shall support the storage of the partial (MM/DD) and/or full (MM/DD/YYYY) date of birth for a person.	✓	✓	✓
REG_0120	PSU	The registry shall have a unique identifier (non-SSN) for each person in its data store.	✓	✓	✓
REG_0130	PSU	The registry shall support the storage of a person's gender.	✓	✓	✓
REG_0140	PSU	The registry shall have the ability to storage multiple net ids for a person.	✓	✓	✓
REG_0150	PSU	The registry shall have an indicator as to which is the primary net id for a person.	✗	✓	✓
REG_0160	PSU	The registry shall store a person's first, middle (optional), last name and suffix (optional).	✓	✓	✓
REG_0170	PSU	The registry shall maintain a history of a person's name changes.	✓	✓	✓
REG_0180	PSU	The registry shall store a type associated with each person's name (for example, legal name). - Does this imply that multiple name types can be stored? (Legal / Preferred etc.)	✓	✓	✓
REG_0185	PSU	The registry shall have the capability to store multiple name types for a person. Examples include: legal name, preferred name, ...	✓	✓	✓
REG_0190	PSU	The registry shall support the storage of multiple addresses for a person, indicated by a type (for example, employee home address).	✓	✓	✓
REG_0200	PSU	The registry shall store for an address, the following information: street address (multiple), city, state, postal code, country, campus location and source.	✓	✓	✓
REG_0210	PSU	The registry shall store for a person's name an flag to indicator whether a first name is unknown (FNU) and/or a last name is unknown (LNU).	✗	✓	✓ Name is blank
REG_0220	PSU	The registry shall support the storage of multiple telephone numbers, indicated by a type (for example employee office telephone number).	✓	✓	✓
REG_0230	PSU	The registry shall store for a telephone number the following information: area/country code, phone number, extension (optional) and source.	✓	✓	✓
REG_0240	PSU	The registry shall support the storage of a person's email address(s) and their respective type.	✓	✓	✓
REG_0250	PSU	The registry shall maintain a history of all of a person's address changes.	⚠	✓	✓
REG_0260	PSU	The registry shall maintain a history of all of a person's telephone number changes.	⚠	✓	✓
REG_0270	PSU	The registry shall maintain a history of all of a person's email address changes.	⚠	✓	✓
REG_0280	PSU	The registry shall support the storage of information about all of the credentials a person holds (for example: kerberos principal, secure id token serial number, PKI, ...).	✓	✓	⚠
REG_0290	PSU	The registry shall support the storage of all a person's affiliations. (Should we add something here distinguishing between affiliations vs. roles per the email discussion)	✓	✓	✓
REG_0300	PSU	The registry shall support the storage of a person's Identity Assurance Profiles.	✗	✓	⚠✓
REG_0310	PSU	The registry shall store information related to an identity proofing event.	✗	✓	⚠
REG_0320	PSU	The registry shall support the storage of identity card information.	✓	✓	✓
REG_0330	PSU	The registry shall either store an indicator or have a calculation to determine a person's primary affiliation.	✓	✓	✓
REG_0340	PSU	The registry shall support the mapping of its affiliations to the eduPerson attributes.	✗	✓	✓
REG_0350	PSU	The registry shall provide a comments facility to be used for authorized personnel (Security) to record information about person's identity.	✗	✓	✓
REG_0360	PSU	The registry shall have complete auditing of information in its registry	⚠	✓	?
REG_0370	PSU	The registry shall provide a facility by which authorized personnel can obtain a read-only view of portions of its data.	✓	✓	✓
REG_0380	PSU	The registry shall maintain a single namespace for person identifiers and network ids.	✓	✓	✓
REG_0390	PSU	The registry shall support the storage of common HR and student information, like title, status and department.	✓	⚠	✓
REG_0400	PSU	The registry shall support the storage of international forms of user information.	✓	⚠	⚠✓

REG_0410	Jasig/OR	The registry shall support the storage of organization-specific attributes.	⚠	⚠	✓
REG_0420	Brown	The Registry shall support the ability to associate a START DATE with each Affiliation type.	✗	✓	✓
REG_0430	Brown	The Registry shall support the ability to define different life cycle processes for removing an Affiliation type (eg staff accounts are disabled immediately; faculty retain their accounts for six months but with reduced services).	✗	✓	⚠
REG_0440	PSU	The registry shall support the ability to associate an END DATE with each Affiliation Type.	✗	✓	✓

- Where do attributes like department / organization / campus fit in the above requirements? Would this be in address and or affiliations or should we be explicit in identifying these things if appropriate?

- Not sure if i missed it or if it is implied, do we have some sort of status indicator? active / in active (in HR terms it might be active, terminated, retired, etc.)

-- many of the attributes that the Registry is required to store (eg email address) strike me as being related to an Affiliation (eg if I'm STAFF and ALUM, I may want to associate different email addresses with those Affiliation types).

-- often there are faculty in senior administrative positions (eg Provost and Prof of Mathematics). Full info (eg telephones, office location) should be maintained for each of these positions that one person occupies.

-- Brown delivers instruction through academic depts; we deliver research via Centers and Institutes. Many faculty/researchers have multiple associations, and even multiple offices.

-- should the Registry be able to store info about Federated Users (eg Jane is a faculty member @ Cornell; she is a member of groups at PSU); same question about people (parents) who authN with Social Credentials to access campus based services (eg Student Bill)

-- do we need requirements related to non-person entries in the Registry ?

DRAFT Requirements (Sept 9 conversation about Affiliate types)

	KIM	PSU	Open Registry
The Registry shall support a LIFE CYCLE model. Each user is in a specific state; incoming events MAY trigger a transition to a new state; entering a new state MAY trigger sending events. Each of these transitions MAY be associated with a different Business Process.	⚠	✓	⚠
The Registry shall support having unique LIFE CYCLE models for each Affiliation type (eg staff accounts are closed immediately on separation; faculty permissions are trimmed on separation but accounts are closed six months after separation).	⚠	✓	⚠
The Registry shall support allowing a site to manage the Rules that define the transitions within a LIFE CYCLE.	⚠	✓	⚠
The Registry shall support optionally sending events whenever a user's attributes or Affiliation types changes.	✗	✓	✓⚠
The Registry shall support a core set of information that is maintained about each person (eg name(s), DOB, citizenship, etc).	✓	✓	✓
The Registry shall optionally support, for each Affiliation type, a scheme that defines the set of information and attributes that will be maintained for this Affiliation type for each user (eg staff have titles and office locations, students do not)	✗	⚠	✓
It shall be easy for sites to modify and extend the schema associated with an Affiliation type (both the data definition step, and adding code to do specialized processing).	✗	✗	✓ ?
The Registry shall come with scheme sets that could be used with different models of Person Registry (eg thin, medium, fat).	✗	✗	✗
The Registry shall provide the ability to have people review and approve changes and transitions via a Workflow mechanism.	✓	⚠	⚠

Management Functions

The section will detail requirements related to management information that the registry should provide. The interfaces will typically be Web Services (SOAP and/or REST-based).

Requirement ID	Requirement Source	Requirement Description	KIM	PSU	Open Registry
MAN_0100	PSU	The registry shall provide interfaces for authorized registry authorities to manage information in its data store.	✓	✓	✓ (Archiving may need refactor)
MAN_0110	PSU	The registry shall provide services to add, update, and archive persons.	✓	✓	✓
MAN_0120	PSU	The registry shall provide services to add, update, and archive address information for a person.	✓	✓	✓
MAN_0130	PSU	The registry shall provide services to add, update, and archive name information for a person.	✓	✓	✓
MAN_0140	PSU	The registry shall provide services to add, update, and archive telephone number information for a person.	✓	✓	✓
MAN_0150	PSU	The registry shall provide services to add, update, and archive net id information for a person.	✓	✓	✓
MAN_0160	PSU	The registry shall provide services to add, update, and archive credential information for a person.	✗	✓	⚠
MAN_0170	PSU	The registry shall provide services to add, update, and archive Identity Assurance information for a person.	✗	✓	⚠✓
MAN_0180	PSU	The registry shall provide services to add, update, and archive affiliation information for a person.	✓	✓	✓
MAN_0190	PSU	The registry shall provide services that are either SOAP and/or REST-based.	✓	✓⚠	✓
MAN_0200	PSU	The registry shall provide a web-based front-end to the data contained in its registry for authorized personnel.	✓	✓	✓
MAN_0210	Jasig/OR	The registry shall provide a flexible batch-file interface for importing and extraction of data, including support for fixed column, CSV, XML, .xls, and other formats.	⚠	⚠	✓

MAN_0220	Brown	The Registry shall provide a means of purging categories of entries (eg Applicants)	✗		✗ or ✓ via expiration
MAN_0230	Committee	The registry shall provide a configurable means by which changes can be (optionally) reviewed and approved	✓		⚠

-- I'm assuming that many of the above process would be built on top of a Workflow system (allowing people to request a change, which is then reviewed and approved) ?

Enterprise System

This section will detail requirements related to the enterprise system aspect of the registry.

Requirement ID	Requirement Source	Requirement Description	KIM	PSU	Open Registry
ES_0100	PSU	The registry shall support the notification of data changes to entities either using publish/subscribe or point to point communications.	✓	✓	⚠ ?
ES_0110	PSU	The registry shall support auditing of all actions for a person record.	⚠	✓	✓
ES_0120	PSU	The registry shall support data reporting of registry data for authorized personnel.	✗	---✓	⚠
ES_0130	PSU	The registry shall notify end-users via email *x* days prior to the expiration of their services.	✗	✓	⚠
ES_0140	PSU	The registry shall have rules for cleansing and standardizing data before its entered into the data repository.	✓	✓	✓

Gap Analysis:

Looking at the current options in the open source space and seeing where there are gaps against the in scope requirements above.

Project Definition - Resources Needed, Outcome Expected, Timeline, :

explore the open source and commercial offerings against our scope and requirements.

Recommendations:

coming after the above