Registries

CO and Registries

What is a registry? What can they be used for? How do the different kinds of registries change to reflect the needs of the CO? Of the enterprise?

At its most basic, a registry is simply a place of record. Complexity enters in to it when one considers what exactly is being registered, where it is being registered, who (or what) is accessing the registry, and to what use the registration will be applied.

In the middleware space, there are two major forms of registries – a Person or People registry, and a Service registry. These registries may cover information in a single institution – an Enterprise registry – or many institutions – a Collaborative Organization (CO) registry. The registry may be recorded in a database, an LDAP directory, a wiki space – there are many possibilities.

	Enterprise	CO
Person Registry	A person registry is a directory or database whose primary functions are identity reconciliation. It is generally pulls its information from institutional ERP systems in to a single database and/or directory. Information is then in turn consumed by institutional applications, with appropriate use agreements in place.	A person registry is a directory or database whose primary function is to collect identity information from dispersed systems of records across multiple institutions for use by a CO. Data collected tends to be minimal, focusing only on need-to-know information sufficient to allow for authorization decisions within the CO.
Service Registry	A service registry provides a normalized "handle" to an application or other software artifact that it can use to access some well-defined resource within its operating context. Having this as a centralized resource allows applications to go to one place to know where they can receive services in the local operating environment, rather than having to query all systems in their space. This record of services can be as broad as necessary to the institution.	A record of services available to the tools and users of a particular collaboration, with a focus on what tools externalize their authentication, authorization, and group management. *This is where the question of what CO metadata needs to exist for collaboration management platform interoperability may come in to play.*

Open questions:

- where does the reconciliation of records occur? Probably needs to occur at both ends. For an enterprise registry, it occurs within the context of the single institution as the information regarding an individual or a service changes. For a CO registry, it is more likely to occur for the individual as someone must reconcile the transition of a person from one institution to the next – there is currently no 'automagic' way to have that reconciliation occur within the CO. Someone, either the user themselves or an administrator within the CO, will need to do something.
- Are these registries directories or databases in and of themselves, or are they an inseparable part of a larger IdM framework? It doesn't make sense to have the person registry be a separate component, but the services registry may be suitable to such a model.

Benefits of registries

Most obviously, registries provide utility by feeding systems that manage identity and services. Beyond that, however, person registries can provide reporting agencies with numbers of participants and locations and other kinds of reports that funding agencies want to see. For the CO, it serves as the integration of campus and CO information. The person registry is the heart where automatic mechanisms can be installed to trigger changes in participant status, e.g. satisfied training, has left the collaboration and wanted records archived, proven citizenship. The service registry is the stepping stone for collaborators to decide what available tools will be the best fit for their particular brand of research. For both registries, there is a self-service component that cuts down significantly on the overhead of managing information, giving the people involved more time and tools to do research.

Person registry story

With over a hundred participants from ten institutions participating in the collaboration, the virtual organization depends on the institution to be the system of record for who is faculty, who is student. The home institution handles the authentication to prove individual identity and does all the updates regarding the status, name, and titles for the individual. All of this information is consolidated from local systems of record in to a single registry that the VO identity management system can query. The VO itself keeps records regarding individuals for name, preferred contact information, and home institution or systems of record. Reconciliation when a person changes information within the home institution is entirely in the hands of the home institution – the VO is simply a consumer of the data. Reconciliation when a person changes institutions is in the hands of the individual and possibly the VO.

Service registry story

Applications are developed over time that allow for externalized authentication, authorization, and group management (bundled together called "application domestication"). As each application has another feature added or modified, it is discovered by a service registry within the collaboration management platform. The CMP will expose those applications as options to the each VO as a possible tool for their collaboration.