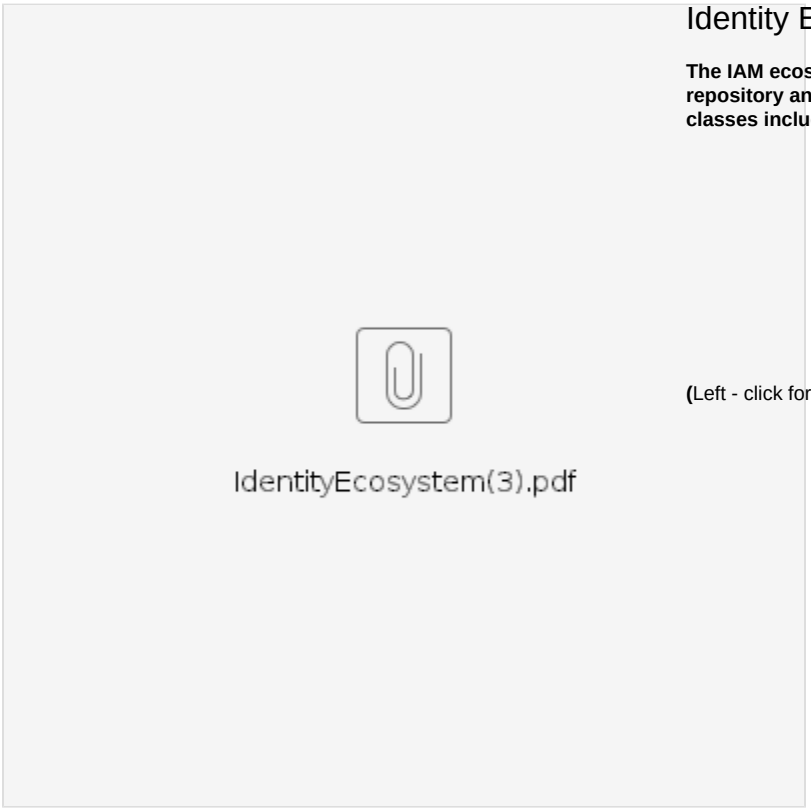
Minimal/Thin Entity Registry

Internet2's Trust and Identity in Education and Research (TIER) program provides a range of core functionality, including group and access management, single sign-on, and federation management. But peering deeper into the layer that forms the basis for Identity and Access Management (IAM) functionality, the TIER Entity Registry Working Group and the TIER Data Structures and APIs Working Group have proposed a data ecosystem required to support the TIER components. Central to this ecosystem is a well-defined strategy for the creation and use of data repositories. These repositories must be complete, flexible, and extensible.

The aforementioned working groups recommend that TIER include a "thin" registry—one which contains the minimum number of attributes that are common to *all institutions' needs* which an individual institution would augment according to its own local needs. This as opposed to a "thick" registry**,** which would contain a rich (but lengthy) set of attributes, with each institution choosing a *subset* to use for its purposes. You can read more about the rationale for this choice later in the blog. First, we need to explore the Identity Ecosystem.



Identity Ecosystem

The IAM ecosystem includes three major data classes in a repository and a fourth supportive data class. The three data classes include:

(Left - click for larger image)

- **Entity registry –** Person and non-person objects that require access management functionality and interface to that functionality.
- **Entity groups and privileges –** TIER proposes, through the Grouper Implementation Guide, a useful strategy for defining groups of securable entities. See the TIER Grouper Deployment Guide for more details.
- **Operational data store (ODS), master data management (MDM), data hub –** Unified and normalized person or entity data concepts an institution elects to manage independent of IAM and useful to many line of business applications**.**

A fourth class of repository information is rules for mappings—and a consistent (normalized) view—across all Systems of Record (SOR).

The registry, group and person data classes can be as thick or thin as an institution's practice allows. The classes do allow for an evolution over a period of time. The TIER Entity Registry Working Group **recommends that the registry remain thin if possible**and be limited to only the information that affects access management related service. The grouping and provisioning structure (such as Grouper) will in turn keep track of all of the relevant groups.

Thick versus Thin

Think about the notion of "IAM is simply another vertical application" with respect to those data hub efforts. IAM should provide data to the hub, and also consume data from the hub, just like other applications. What are the advantages of a minimal/thin registry?

- Avoids rebuilding an operational data store or master data management structure that may already be in place or on the institutions strategic path. Uses it as a component of the repository.
- Uses a common person (subject) data hub that is available to all applications is becoming more prevalent. This can be leveraged by the IAM application as well.
- Enables agility and flexibility downstream.
- Reduces the amount of personally identifiable information in the registry.
- Enhances security - Access data only needs to be shared with those with a need to know. Exposure of data is less.
- Enables groups and provisioning in a Role-Based Access Control (RBAC) or Attribute-Based Access Control (ABAC) model is better if driven from a Grouping /Provisioning tool (Grouper, Midpoint, etc).