Minimal Entity Registry Definition/Logical Design

The idea of minimal person data in the registry is driven by requirement # 10 and the idea that the data repository for IAM is comprised of a registry, a group and a ODS/MDM person data repository. Data for IAM operations can go to or be brought from the virtual combination of these three data repositories.

This is a final DRAFT doc. Review is in-progress by TIER WORKGROUP

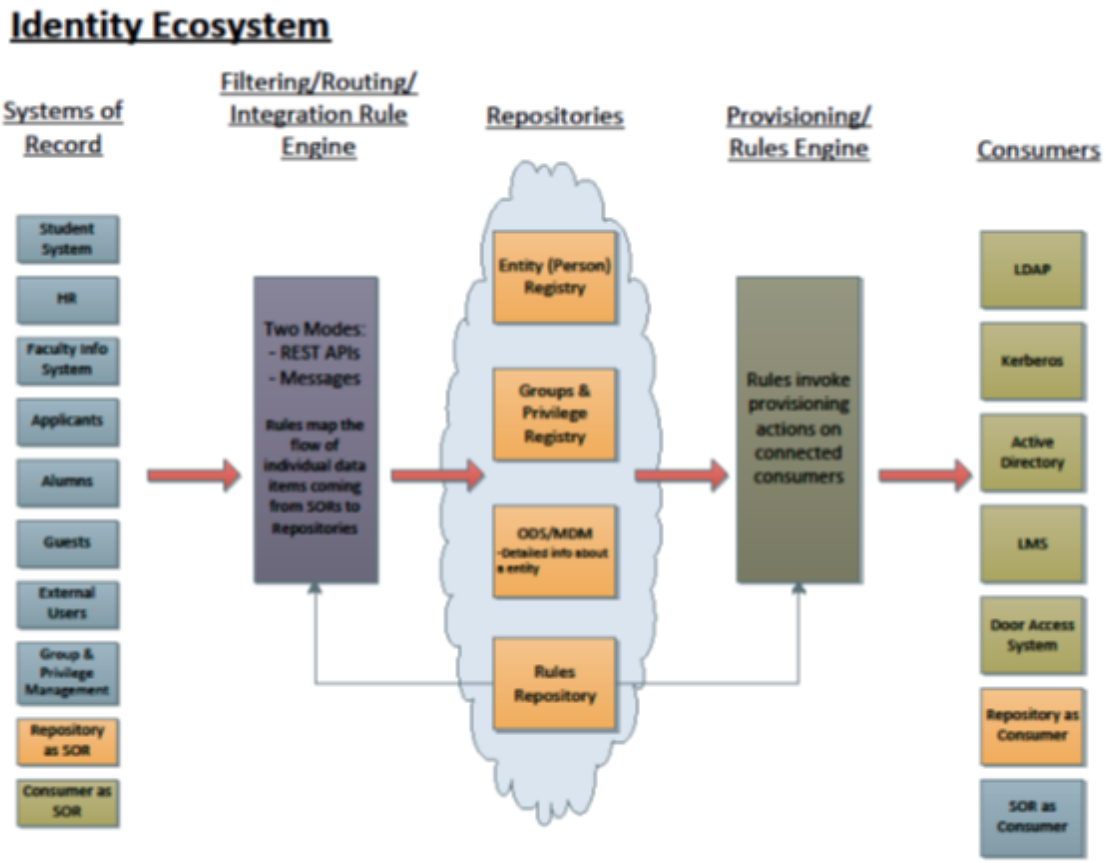

Diagram from May 2016 TIER Entity registry documents.

The three data classes defined include:

- **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 from the systems of record “Basis Groups”, transformational abstractions into Reference Group forms then relating these to form Application related permission groups. See the TIER Grouper Implementation Guide for more details.
- **ODS, master data, 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**.**

Why propose a minimal/thin Registry?

- Avoid rebuilding an ODS or MDM structure that may already be in place or on the institutions strategic path. Use it as a component of the repository.

- Use of a common person (subject) data HUB that is available to application is becoming more prevalent. This can be leveraged by the IAM application as well.
- Agility and flexibility downstream.
- Reduce PII and other privacy implications in the registry.
- Isolate the access management info and the growing aspects federation from the more data rich environment of the data hub.
- IAM is a SOR for Access management info. So for same reason we have other vertical applications that use a common reference data the IAM Registry can be thought of in the same manner.
- Security - Access data only needs to be shared with those with a need to know. Exposure of data is less.
- Groups and Provisioning in an RBAC or ABAC model is better if driven from a Grouping /Provisioning tool (Grouper, Midpoint, etc)

Why not use a thick registry?

- Generally does not scale as well as thin designs
- Produces more data duplication and with other services (like ODS or data hub).
- Duplication of efforts and talent in your IT organization
- Efforts to build thick registries can create complexities and related operational problems.
- More risk based on projects undertaken in the past

This document focuses on TIER PERSON and TIER CLIENT entity can be extended to document other supported entity types.

Requirement Document located for TIER registry and other TIER components at Requirements on an Entity Registry and Related Components

Entity Object- person, institutional contact, code client (thing calling API), service/privileged acct, IOT(device), etc.

- Each occurrence will have a unique identifier assigned to identify it for use in the IAM architecture to uniquely know this "thing" from all other "things".
- This requires a high level structure in the data to provide uniqueness for all entities.
- In the case of matching, merging of suspect records this is a key capability.

==========

Entity Data Definition:

- used for all type of entities

- **Entity object ID**
  - internal
  - used internal to registry only
  - UUID type of value
  - Key value for any registry entry
- **Entity Type Code**
  - Person
  - Client/Service
- **Date created**
- **Date Inactivated**
- **Entry Description / Name**
- **Status**
  - (suspect, merged, active, inactive)
  - Inactive = soft delete
- **Institutional Entity Identifier**
- ***Object Maintenance Fields*** *(rather than show this at each object or field this is shown once and can be applied to any object and /or field))*

  i. ***Begin Time Stamp***

  ii. ***End Time Stamp***

  iii. ***Updating entity ID***

  iv. ***Updating SOR*** *Identifies SOR (or Business area) of last update*

Entity Type: person

- **Person object:**
  - **Protect/Secured**
    - Definition – Person entity is accessible or is protected from exposure, although a more robust solution for privacy could be extended to each/all lower level object or fields this is the minimal level. Person on/off.
    - Requirement(s) – Allowed values are "Y" or "N"
      - Additional Information - Person information may not be public because of person preferences or for legal protection reasons.
      - There are persons with specific security roles that have access to Protect/Secured information.
      - Specific roles have maintain authority Protect/Secured.
  - **Active, Inactive and Pending Status**
    - Definition – The state of the Person record for usage by authoring systems
    - Requirement(s) – value must exist in code table
    - Additional Information:

- "Pending" indicates that an identity resolution event is underway
- "Inactive" indicates that the record did not survive the collapse/merge process a new record exist
- "Active" indicates that the record is to be used for common business usages

- **Identifier Object** (At least one occurrence is required many are allowed per institutional need**, "**Institutional Entity Identifier" from the Entity object must reside in person identifier have used a bunch of examples (these can vary per institution)
  - **Identifier Type Code** (bold types are minimal required)
    - SOR owned
      - **Institutional Identifier**
        - Registry is the SOR
        - only required identifier
        - requirement 4 would return the institutional identifier value to the calling client / SOR
        - other examples for etension are below in RED
      - "ANY SOR ID" - extend as needed for HR, SIS, BANNER or whatever, SOR level is recommended strongly for all SOR with a reference identifier.ORCID -- needs to be provided by the ORCID organization; there is a format that is required;
      - ERA Commons ID -- no special editing; for National Institute of Health
      - NSF -- no special editing; National Science Foundation
      - ID Card NO – no special editing; card ID for a person
      - Library ID -- no special editing; Library Number
      - Door Badge ID-- no special editing; SOR is ID card interface
    - Access management identifiers
      - (USERIDs various net id local or federated, it would be expected that one of these would be present))
      - **UserName** -- no special editing; Highly recommended
      - federated login identifier(s)
        - eppn or similar federated id of choice.
  - **Name object (**Structure Occurs at least once but may be multiple per Person entity (1-M))
    - **Name Type**
      - Definition – Name of the person. Tier Minimal registry requires two specific types of names to be available for entry. One should always be contained in the person info. Both being present is even better.
        - **Legal -** Name associated with gov't documents such as Driver's License, Passport etc. This implies info has been vetted for the person.
        - **Preferred Name** - Name provided with little or no vetting and often desired by the user.
      - other possible types Former, Alias, etc
      - Institutional control in adding types
    - **Formatted Name**
      long string that contains the name parts all combined into a single string value
    - **First Name**
      - Requirement(s):
        - Value is required
        - Fail transaction if null
    - **Middle Name**
      - Requirement(s):
        - Optional – Null allowed
    - **Last Name (Surname)**
      - Requirement(s):
        - Value is required
        - Fail transaction if null
    - **Prefix**
      - From a code Table
    - **Suffix**
      - From a code Table
  - **Contact Method Email Object**
    - multiples allowed
    - 1 required
    - **Primary**
    - **Email Type**
    - **Email Address**

- **Contact Method Telephone Object**
  - multiple allowed
  - 0 required
  - Basic Phone International Rules apply
  - **Primary**
  - **Type – Maintain the type of device (example types are Wired and Cell)**
  - **Telephone Number – Full number is to be stored**
    - **Country Code**
    - **Area Code**
    - **Telephone Number**
    - **Device Type**
    - **SMS Capable**

Entity Type: application (represent a thing that calls a TIER API)

- **application object:**
  - **Identifier ID**

        - Institutional Id – required for all client objects
    - **Contacts 1-m** (who can be notified for any actions about this client)
        - Identifier - EPPN
        - Name - friendly name
        - Email -
    - **Sponsor**
        - identifier: a permanent (friendly) unique identifier
        - name: friendly name
        - sponsor: Id of the sponsor of this sponsor. (Null iff the root sponsor)
    - **Service**
        - identifier: a permanent (friendly) unique identifier
        - name: friendly name
        - description: Human readable description of this service.
        - sponsor: Id of the Sponsor of this service.
        - admins: list of administrators (eppns usually)
        - contacts: list of Contacts
        - base URL: host, port, base path
        - authns: list of authentication methods supported
        - authorization service: Service of OAuth authorization service (if OAuth supported)
    - **Client**
        - **identifier**: a permanent (friendly) unique identifier
        - **name**: friendly name
        - **description**: Human readable description of this client.
        - **sponsor**: Id of the Sponsor of this client.
        - **admins**: list of administrators (ePPNs usually)
        - **contacts**: list of Contacts
        - **redirect urls**: list of redirect_url (if OAuth supported)
        - **host**: if known and constant.
        - **long-term authentication credential**
            - to itself for each client in its registry.
            - A service will generally authenticate to the CSR with its InCommon certificate.

Audit trail : or similar mechanism is required to be able to review and look at all changes to data.

- entity, attribute identifier, verb, old value, new value, timestamp of change (example)
- should be able to trigger an update notifications/events to Provision when an “attribute” changes on a Person record
- this can vary based on the specific implementation of this design

---

Additional info for Virtual Organization consideration:

Notes on support for VOs and collaborations wrt Minimal Entity Registry Data

Requirement #57

Support for collaborations (as provided by central IT) can broadly be segmented into two categories;

"Simple" collaboration needs cover researchers on campus (ie: those who have campus NetIDs) collaborating with others on campus via access to campus managed services (email lists, documentation spaces, etc). In general, this functionality can be provided with a combination of (existing) group and person registry services, often with a minimal "service enablement" layer to allow authorized individuals to define the collaboration groups and map them into enabled services.

"Advanced" collaboration needs expand to include researchers not affiliated with the campus (ie: those who would leverage federated identity to participate), complex enrollment procedures (invitation, self signup, approval, etc), larger collaborations with delegation requirements, and finer grained service management. Meeting these needs often implies solutions like COmanage.