TIER Entity Registry Working Group

TIER Entity Registry Working Group Home

Call Schedule

- **Wednesdays, 3 pm Eastern, Noon Pacific, 8 pm UTC**
  - video: https://bluejeans.com/678543210/browser
- **Fridays, 10 am Eastern, 7 am Pacific, 4 pm London, 5 pm Amsterdam**
  - video: https://bluejeans.com/678543210/browser

Agenda for upcoming WG meetings plus meeting notes for the past ones are here: http://j.mp/1PWMCp5

Attendees are encouraged to participate in live-scribing the meetings on the above Google doc.

Email List: tier-entreg@internet2.edu

– To subscribe, browse to https://lists.internet2.edu/sympa/admin/tier-entreg

Working Group Co-Chairs: Warren Curry, University of Florida and Benn Oshrin, Spherical Cow Group

Charter for the TIER Entity Registry Working Group

MidPoint as Entity Registry: Investigation and Evaluation

TIER Vision and Overview

- Help education and research organizations solve the Identity and Access Management (IAM) challenges they encounter
  - By providing open source implementations of key IAM capabilities and assuring their long-term sustainability
  - By standardizing
    - How applications (whether local, federated or SaaS) *integrate* with IAM infrastructure
    - How existing institutional IAM infrastructure can *interoperate* with TIER components to provide a full IAM service suite

TIER Entity Registry and Data Structures and APIs Working Groups

- The TIER Entity Registry Working Group and the TIER Data Structures and APIs Working Group share the following key goals
  - To define integration and interoperability strategies and models
  - To help charter development projects that address specific gaps in existing open source IAM packages
  - To develop a comprehensive functional model of IAM
  - To define and adopt specifications for the resource schema and interfaces needed to deliver identity and access management (IAM) services
    - Between the various TIER IAM components
    - Between TIER components and the rest of the institutional IT landscape, both on premise and in the cloud
  - Provide guidance on building IAM infrastructure and processes that accord with the TIER model

Standards, Tools and Guidelines set out in TIER Release 1

- Expose IAM capabilities at RESTful endpoints
  - ...Where it makes sense: LDAP, SAML, etc. still have their well-earned place, TIER will take full advantage of such common protocols and interfaces. OAuth 2, OpenID Connect and UMA are also coming into play.
  - *REST*-ness in the TIER context means: HTTP verbs operate on Resources (groups, users,....); RPCish idioms should only be used when nothing else will do what needs to be done.
  - The model for interoperating with existing institutional IAM services is to provide the TIER components with connectors that know how to interact with both back end legacy systems as well as the growing number of contracted-out SaaS and PaaS services
  - An API-first design helps us achieve and maintain a level of abstraction from specific implementation choices. This gives TIER adopter sites the option to wrap their favorite legacy IAM service in a TIER API knowing that it will integrate well with other TIER or TIER-compliant packages.
- Adopt the many useful conventions specified in the new IETF standard, *SCIM 2.0* ,
  - around the design choices that would otherwise tend to provoke endless working group debates on matters such as pagination, metadata schema, data formats, etc.
  - the choice to leverage SCIM, as much as anything else, made the decision to support *JSON* easier. Support for XML can be provided if and where it's needed.

API Specifications:

- The canonical specification language for _ HTTP-oriented APIs in TIER is *Swagger 2.0*
- Why Swagger and not *RAML* or *API Blueprint*? (see this recent comparison on dzone)
    - In the move from version 1 to version 2, Swagger incorporated a lot of RAML's best features (around reusable definitions, etc.)
    - Swagger 2 has been adopted as the basis for further development by the industry-launched *Open API Initiative* (http://openapis.org, more on github here) and that should strengthen the already thriving Swagger developer and adopter community

TIER Entity Registry Update - 2017 GLobal Summit

TIER Identity Data Ecosystem2col.pdf

TIER Application View Integration Layer Concept of Person Maintenance and Retrieval (Draft)

whc, 11/07/2017

- For use by SORs to retrieve and maintain information related to a person entity.
- For use by any consumer application to acquire information related to a person entity
- 2017 Tech Ex Summary - Registry Summary techex 102017.pdf
- Diagram



- Application that is an SOR needs to indicate to the Identity System there is a new or changed person
    - It would invoke the Maintain Person logic that encapsulates the (Minimal registry, Affiliation and perhaps other groups, and other person data that the institution has defined beyond the minimal registry)
    - The service: validate the use of the service by the calling party/application
    - Person Schema (encapsulated version)
    - The service maps the data from the encapsulated schema into three subsets:
        - registry
        - groups
        - person detail
    - The service call the Registry rest call (Ethan K demo work)
    - The service call the Group rest call (grouper API)
    - The service call the Institution supplied Person rest call (need a sample)

Key Deliverables from TIER Release 1

Requirements on an Entity Registry and Related Components

COmanage / Entity Registry Gap Analysis

IAM Functional Model and IAM Glossary

TIER Core Schema for Systems of Record and Entity Registry - Early Draft

Narrative Form: Deliverables in the WG Charter

1. Document *Functional Requirements for System of Record (SoR) to the Entity Registry* Define a minimal first iteration *Registry person schema /resource*
2. Draft *a first iteration functional model for IAM with a glossary of institutional processes around identity lifecycle management* .
3. Draft *fit/gap analysis between current COmanage registry functionality and this WG's Entity Registry requirements* .
4. Provide COmanage Team with *rough definition of work required to fill gaps in COmanage functionality*

Entity Registry Requirements

- From CIFER Registry Team
- From CIFER Enrollment (Registration) Requirements
- From TIER campus surveys
- From U Florida (courtesy of Warren Curry)

Functional Model for Entity Registry and Allied Services

- Identity Registry Functional Model (Sept. 2011, CIFER)

Schema for core IAM resources

- Prior work: CIFER SOR-Registry Core Schema Specification
- Gabor's overview: https://gist.github.com/geszes/3d4b9ff49441058db434
- Draft Based on Schema.org: https://gist.github.com/geszes/6bfd8926bded03786a63
- Clemson Authology schema: http://authology.org/doc/VaultServiceReference/vaultServiceReference.html
- Penn State Person Bio Record
- COmanage Registry Data Model
- Person Schema Comparisons:
    - https://spaces.at.internet2.edu/display/cifer/SOR-Registry+Core+Schema+Strawman
    - https://gist.github.com/geszes/a889d023a3a26a763c6f

Member-contributed Resources

- University of Wisconsin - UDS Person Schema
- Comparison of UW-Madison UDS Person API and CIFER API
- Rob Carter thoughts on fine-grained authZ on APIs for data access

---

See Also :

- TIER Working Groups Home
- TIER Data Structures and APIs Working Group
- Background information on TIER , Internet2 initiative on Trust and Identity in Education and Research