Evaluation of midPoint against TIER Requirements on an Entity Registry and Related Components

General Principles

1. Support/advertise a strong conceptual difference between email and user ID
2. Support widely used standard authn/authz protocols for federations (OAuth2 + SAML2)
3. Support multi-site replication and synchronization
4. Support unicode (and make clear what character set is supported)
5. Avoid/disallow re-use of persistent identifiers (or define “persistent” better!)
6. Allow non-person Entities
    a. Client /Agents
    b. Service Accounts
    c. Department/Organization
    d. Internet of Things (devices, IOT)
7. Suggest various ways people can model their data; Do we want a registry that could host different models?
    a. Relational vs LDAP
    b. Use as delivered vs. customize
    c. “Built in” schemas vs. common configurations (that can be customized)

Companion Doc for Data minimal requirement for items marked registry Minimal Entity Registry Definition/Logical Design

Tabulated Requirements

#	Component	Requirement	Notes
1	**Identity Registry**	1. Paths in and out 1. RESTful API 2. Asynchronous messaging interface (PUB/SUB, etc) 3. Administrative interface console	1.1 Yes 1.2 No (coming) 1.3 Yes
3	Identity Registry	For new records, assign a permanent unique identifier to map between various source system identifiers. This entity identifier must be made available to the SOR as a response to the entry from the SOR.	Yes
4	Identity Registry	When SOR notifies Registry of an entity/person, the Registry should return the unique identifier that the registry is willing to share externally. The institution may extend what is returned (?)	?
5	Identity Registry	Change (add/modify/delete) notifications/events to Provision when an “attribute” changes on a Person record. Minimally registry records entity, attribute identifier, verb, old value, new value, timestamp of change	Yes
6	Identity Registry	An entity/person can have multiple simultaneous affiliations with an organization. We will use the term affiliation	Yes
7	Identity Registry	Each relationship has a “type” (affiliation) and can have its own set of data describing ~~the individual and~~ this relationship (start/end dates (possibly in the future), dept/center, ~~title(?)~~, who/what added the entry, affiliation type owner); this is data about the 'membership', not about the person who is the member	? This speaks to the need to have, say, membership create date ~~phone # associated with a specific affiliation~~
8	Identity Registry	An entity can have multiple affiliation relationships with the same "type" value (eg faculty member who is associated with multiple academic departments)	Yes.
9	Identity Registry	Support start and end (sunrise/sunset) dates for attributes. Many attributes should support these dates. Phone, email, name(s), affiliations, etc. The date serve as triggers and allow for a live history to be built for an entity.	~~? BPM could handle,~~ this is all available in the audit logs
10	Identity Registry	The Registry does not need to hold all IAM data within it. Rather data is to be considered to be contained in one of three conceptual data containers: Entity/Person registry, Groups and Privileges, Party (person/organization) ODS/MDM data stores.	NA
11	Identity Registry	Support extensible local and/or auxiliary information about entities	Yes
12	Identity Registry	Associate a “level of confidence” with various attributes (eg self-asserted, verified via gov’t documents, etc)	metadata on attributes or SoRs; no V1 support (at most, trustworthiness of authoritative source of data)
14	Identity Registry	Email notification to user indicating change/pending change to key registry profile information. (data awareness vs data management)	? Need to find out. pass a file of needed changes

15	Identity Registry	Support Batch purging of entries (e.g., applicants) [May require a different concept than "purge". "Permanent disable"?, should use a soft delete mechanism]. Generally this will be the ending of an affiliation like applicant it might even add an affiliation former applicant. A repetitive calling of the API/message (see #1) is the process or doing this. Institution would set up a process to take in a list and call the service. This assures that edit, triggers and all logic involved in setting individuals and communicating changes is followed.	? Batch "Staus" for soft delete?
51	Identity Registry? Access Management?	A Person may have multiple personas that an organization may require them to “act in the role of”, An easy way of switching personas should be constructed as a part of the final solution. Really an acccess management issue	manage with authZ groups? Application specific; Limited registry use case around workflows (e.g. approving request as an X vs Y
35	Identity Registry	Associate multiple authentication methods with an entity in the Registry; ability of UW System students to use credentials from any school they are connected with and be recognized as the same person	?Account linking; Outside systems could handle non-mP authn methods
36	Identity Registry	Methods can be internal (ie managed by the organization) or external (ie rely on a different organization to perform the authentication and assert its result; eg social)	Yes, but check. (Federation support); related to #35 above
37	Identity Registry	Each Authn method should have an associated LOA - Assurance measure/value (support for MFA	? Grouper as a tool
61	Identity Registry	Support various management models for GUEST types (eg self-registration, require a Sponsor with specific Roles, etc)	Capability to support is there;
62	Identity Registry	Support specific terms for GUEST type (eg must be renewed every N months)	Yes
57	Identity Registry	Ability to spin up "collaboration services" for campus researchers and other groups, where a campus member is designated as the collaboration administrator and can invite other participants, and can enable applications (such as file storage and email lists) for the collaboration.	Yes via group-based provisioning; check with Benn;
56	Audit	Ability to store comments associated with any identity and access management edits (including running comments); any time there is a manual change to registry data there should be support for a comment.	Not V1; sophisticated logging infrastructure required, or application level support. JonF has an "Operational Comment" facility that a number of differnt applicaitons use to make "comments" on a person (entity). Some of these are generated as part of other processing and others are done manually. These entries can optionally have a "due date" and a "pending" flag. These are sorted by "Family". genertes alerts for "pending" entries to the appropriate contact. For example, when an employee is terminated, and an asett delegate selected, two comments are generated for the postmaster to share the email and 30 days later to remove the mailbox share
2	**Identity Registry** **Identity Matching**	As part of Registration from an SOR, invocation of Identity Matching Engine . Registry attempts to match with an existing record • match - can positively identify an existing Registry entity /person - becomes an update • no match - Can not identify a preexisting registry entity/person - becomes and add • indeterminate (maybe) identifies possible collisions but match logic is not scored high enough to determine a specific match. This requires a human interaction and mapping of information. A new record will be added with a "suspect duplicate status" . A data steward (human) type responsibility to resolve these using the merging/splitting function. The institution will need to decide if provisioning is allowed to these cases prior to resolution. It is the working groups recommendation that these suspect duplicates are not candidates for service provisioning until they are resolved and no longer a suspect duplicate record.	deleted former 17 and 18 row duplicate to this. ? Identity matching is required function. Might be a service call to a Identity match service , Solution to be determined,
47	Identity Registry Identity Matching	Support for finding potential duplicates ("suspect duplicates") entity /persons and adding/merging/splitting records to resolve and the resolution of these registry entries.	Moved to pair with the requirement - matching function item # 2; can be reflected in Grouper
19	Identity Registry Identity Matching	Identity merging needs to be well managed and low impact. The assignment of provisional ids is a method for special use cases of merging	Id Match functionality and mark identity as suspect;

20	Identity Registry Identity Matching	Attempts to match with an existing record in the Registry use heuristic algorithms	ID Match function
21	Identity Registry Identity Matching	May rely on “attribute assurance level” when matching input values against Registry entries	e.g. Self-asserted vs SoR authority at attribute level mP: Scripting of attribute resolution
42	**Identity Registry** **Audit**	Events performed by any of these components must be recorded such that an Audit system can perform queries in various ways and see the results of those queries	See 56 above, must be easily retrievable; mP provides ability, check customizable
43	Identity Registry Audit	Maintain a secure permanent audit record / history of ALL changes related to an entity record.	Configurable
32	**Identity Registry Authentication**	Users must be able to authenticate to the Admin Console	Yes
33	Identity Registry Authentication	The Registry should support authentication via CAS and Shibboleth (SAML2) or other methods supported by TIER. The Identifier provided by the authentication mechanism should be used to search the Registry to find the matching record.	CAS yes, Shib worth testing
34	Identity Registry Authentication	External services must be able to authenticate to the RESTful /messaging endpoints exposed by the Registry	API Security capability, UN/pw
53	Identity Registry Authentication	Beyond WEB Only Authentication (e.g. ECP and CLI protocols) for authentication must be enabled as for Research/Collaborative computing	Not registry function; Make sure it doesn't prevent non-web authN; investigate
40	**Credential Mgmt /Storage**	Provide a mechanism for (possibly) storing and propagating various secrets supporting authentication (eg passwords, personal certificates, two-factor secrets, lower quality passwords (eg synched gmail), KBA questions/answers	Check; KBA?
41	Credential Mgmt /Storage	Password Reset capabilities must be standardized upon and deployed in the out of the box solutions, with sufficient flexibility to meet institutional business practices. (Probably need to talk through the non-password self-service interface --)allow emailed one-time links, one-time printed tokens, 2FA and other "private token" mechanisms)	Yes; Provide details
38	Credential Mgmt /Storage	Various events can raise and lower the associated LOA (eg password reset over the phone could lower a password-based LOA)	?
39	Credential Mgmt /Storage	If an internal method has Identity Vetting Requirements support them in some fashion	? Possible with Grouper;
49	Credential Management	Support for out-of-band password reset mechanism ,(SMS/email, etc)	?? huh?
13	Credential Management	Provide a mechanism for (possibly) storing and propagating various secrets supporting authentication (eg passwords, personal certificates, two-factor secrets, lower quality passwords (eg synched gmail), KBA questions/answers	== #40
45	**Identity Registry** **UI Console**	Search for users (including users who are no longer active)	Yes
46	Identity Registry UI Console	Support for “renaming” users, and changing any of their attributes (including their various identifiers)	userId changes supported?
48	Identity Registry UI Co nsole	Support for creating entities in the Registry	Yes
50	Identity Registry UI Console	Support for authentication to Admin console using various authentication methods	Yes

54	Identity Registry UI Console	Allow users to see (portions of) their records, and maintain the self-asserted attributes in their record	? end-user role configuration
16	**Groups**	There is a need to identify a “primary” Affiliation? (Primary affiliation calculation is a requirement to assist in handling the EduPerson Primary affiliation., calc required when individual has multiple distinct types of affiliation student and employee for example institution must decide how they handle this.	? Does mP support a role conflict resolution mechanism?
52	Groups	Support for authorization framework (different People/Roles authorized to see/change different attributes; LOA of authentication method affects permissions)	Yes re multiple role and permissions, but no re differentiating access on AuthN strength, perhaps with more sophisticated access policy tools (support for conditional permissions)
60	Groups	Provide support for the creation and maintenance of a type/affiliation of “GUEST” affiliation and many others on Registry records	Yes.
23	**Provisioning**	When an “attribute” changes on an entity data was placed for provisioning to consume based on the event. Entity record an event to be provisioned with minimal field including: entity, attribute identifier, verb, old value, new value, timestamp of change.	Yes, with some development work
24	Provisioning	Rules that specify Provisioning Operations can trigger these events (invoking specific outbound Connectors associated with specific target systems)	Yes, with some development work
25	Provisioning	These events can be consumed by internal processes which then change other Attributes (eg passing an End Date causes Status to change Active to PENDING)	Yes, with some development work
26	Provisioning	These events can also be consumed by “Connectors”, which then effect changes in external systems.	Yes, with some development work
27	Provisioning	Semantics of a change are determined by each Connector (eg ldap vs google vs LMS, etc)	Yes
28	Provisioning	Receive from the Provisioning System an event describing a change in the Person record; they map that change to the appropriate sequence of events to transmit to their associated external system. (eg provisioning accounts, synchronizing passwords, changing permissions, etc)	Yes
29	Provisioning	Events contain: attribute identifier, verb, old value, new value)	Via scripting
30	Provisioning	A mechanism to augment the catalog of Core Connectors must be provided to the community for inter-institutional sharing and implementation.	Yes.
31	Provisioning	A set of pre-built connectors should be supplied “out of the box” (eg ldap, AD, kerberos, Grouper, SCIM, some popular cloud based services (eg Canvas), etc), Initial for LDAP, Kerberos only	Yes. Supports all ConnID framework connectors plus custom connectors
44	Provisioning	It MUST be possible to see the relationships between events in the different components (eg a Registry change triggers a Provisioning change triggers a Connector action)	Yes, with some development work
55	Provisioning	Support for workflows that involve administrative sign-off from specific users (eg approval for certain types of edits)	Yes
58	**Consent**	The solution may enable user to be in control of their personal data stores such that when relying parties are requesting access to those data, users should have fine-grained controls over what pieces of personal data are shared with such parties.	Not a registry function, but Shib supports 'consent-informed attribute release' (CAR). With some development work, connectors could be taught to reach out to a CAR service.
59	Partitioning	Partitioning is mentioned in several use cases, and is difficult to define. There are a number of underlying conditions that seem to lead to "partitioning"; these should probably be teased apart and treated individually, as none of them yet seems compelling on its own. (Most seem like a data presentation question - perhaps a locally defined attribute for an account which is then important when Connectors are invoked).	???? Look back to use case documents to understand what 'partitioining' means.
63	**Community Documentation and Interaction**	Solution extensions must be available in the form of a Marketplace or some other suitable means of presenting a catalog of available functionality, contributed by the community, for utilization by others.	Yes for connectors via ConnID connector framework
64	Community Documentation and Interaction	Solution must enable the sharing of a common documentation repository as well as a place for school practitioners and service providers to go to find useful instructions, standards, practices and guidelines for building end-to-end services based on TIER components	Provided across the TIER components
65	**Standards and Enforcement**	The program must assert and enforce Policy Standards	Csn be configured to do so via policy configuration.

66	**Policy and Performance Monitoring**	Log files should be available to monitoring tools. Should be able to discern what data was seen and changed during a session, Which features were used..	Audit log has much of this information, but it is stored in the mP database rather than going to a log file. Log files are accessible to common log processing tools