Chapter 4.
Identity Vault Requirements

Identity Vault. This includes the Registry and Directory, which serve as the data and processing hub for identity management, service provisioning, and workflow. The modules of the Identity Vault subsystem are:

- **Registry.** The restricted-access collection point for person identity data from institutional sources (such as human resources, student, and development systems), including the Sponsor System. It is the point of all person identity creation.

- **Directory.** An accessible directory that contains active person and non-person identity data, roles, and groups for the purpose of provisioning IT resources.

- **LDAP Tree.** An LDAP-accessible directory instance.

We are also including here the requirements for the components of MCommunity that support the ID Vault, such as the User Applications and Workflow.

Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>What Is the Identity Vault?</td>
<td>1</td>
</tr>
<tr>
<td>How Will It Be Used?</td>
<td>2</td>
</tr>
<tr>
<td>Business Requirements</td>
<td>2</td>
</tr>
<tr>
<td>Operations Requirements</td>
<td>4</td>
</tr>
<tr>
<td>Dependencies</td>
<td>5</td>
</tr>
<tr>
<td>Questions, Future Enhancements, and Design Considerations</td>
<td>5</td>
</tr>
</tbody>
</table>

What Is the Identity Vault?
The Identity Vault is the hub of the MCommunity system. It comprises a Registry and a Directory, including an LDAP accessible directory instance. In addition to these major components, there are subsystems that support the functionality of the Identity Vault. They include the User Applications
(which provide web-based and programmatic access to identity management functionality), Workflow (a collection of internal data-processing mechanisms), and a collection of connectors that exchange data with institutional sources and down-stream IT systems. Requirements for these supporting sub-systems are included in this document as well.

**How Will It Be Used?**

The ID Vault will house identity data for populations such as students, faculty, staff, and alumni—as defined by the Governance Board. This data will be provided by institutional sources and maintained in the Registry using connectors and APIs. Business logic will be employed to present the current population in the Directory with the data needed to provision IT resources. Connectors and LDAP applications will use data in the Directory to make IT resource provisioning and access decisions.

The Identity Vault will have a web-based user interface for creating, viewing, and modifying identity data; defining and managing groups and roles; delegating access to identity, group, and role data; and interacting with the Workflow system.

The Identity Vault is not a provisioning system. It contains and manages identity data but does not assign resources. The Provisioning tools/logic will allow resource owners to define and implement the criteria for which access to resources is granted and revoked based on identity data.

**Business Requirements**

These business requirements focus on meeting the needs of unit IT staff, unit administrative staff, and end users.

**For End Users (Interactive Access)**

1. The ID Vault will provide anonymous access to minimal identity data.
2. The ID Vault will provide authenticated members of MCommunity with appropriate access to identity data based on Governance Board guidelines and policy.
3. The ID Vault will employ measures to prevent data mining by unauthorized entities.
4. Granular privacy controls that adhere to Governance Board recommendations will be provided.
5. The ID Vault will facilitate the creation and management of user groups and departmental roles.
6. The ID Vault will provide a facility for self-initiated uniqname creation and selection for eligible members of the community. This includes alumni, as well as students going through the Office of New Student Programs (ONSP).
7. The ID Vault will provide a facility to communicate assigned uniqnames and UMICHER Kerberos passwords directly to the recipients.
8. The ID Vault will support fuzzy searching.¹
9. The ID Vault will support addressbook application access to Directory data by populating and indexing the attributes required to satisfy popular default configurations used by such applications as Outlook, Thunderbird, Mulberry, and so on.
10. Institutionally maintained and personally maintained identity data will be clearly distinguished.
11. Individuals will be able to modify aspects of their own identity data that are deemed to be under their control, but they will not be allowed to modify institutionally maintained data.
12. Individuals will be able to display group membership and ownership.
13. Individuals will be able to create, manage, renew, and delete user groups.

---

¹ According to Wikipedia, fuzzy searching is the name that is used for a category of techniques for finding strings that approximately match some given pattern string. It may also be known as approximate or inexact matching. Using fuzzy searching, for example, a search for “Gene” would return “Gene,” “Jean,” and “Jeanne.”
14. Individuals will authenticate as themselves to gain access to all the functionality they are authorized to use. This means, for example, that they will not need to authenticate as a security object, as they do now with the U-M Online Directory, to get elevated access for certain job-related tasks.

15. A Workflow facility will be provided for identity management and IT service provisioning purposes.

16. A Workflow facility for inviting people to create uniqnames and for processing the invitations will be provided.

17. Command line utilities that authenticate using Kerberos and PKI will be provided. This includes GSSAPI, Kerberos Simple Bind Proxy, and X.509 mutual authentication.

18. An interface for requesting, registering, and managing umich schema namespace extensions and OID assignment will be provided.

**For System Administrators (Programmatic Access)**

19. The Identity Vault will act as the “one-stop shop” for all identity, group, and role data for the institution.

20. The ID Vault will provide facilities and services to support a central, comprehensive, identity management infrastructure that supports the distributed needs of the entire University community.

21. It will act as the authoritative registry of umich schema namespace extensions and OID assignment.

22. The system will provide the ability to track non-person identities in the Directory, which could include system-related identities or other types of directory objects (for example, rooms, hardware, networks.)

23. Any of the official data sources will be capable of creating a new identity.

24. The ID Vault will employ extensive and effective identity matching and duplicate avoidance techniques to reduce or eliminate creation of undesired duplicate identities in the system.

25. It will allow for extensibility of the Directory Schema to meet departmental needs.

26. The ID Vault will provide the ability to notify down-stream systems of pertinent changes to Directory data in real time based on well defined benchmarks.

27. A foundation for future enhancements will be implemented. Future enhancements might include federation efforts, such as Shibboleth and InCommon; SAML-based efforts, such as Liberty Alliance or local and generic SAML implementation efforts; and PKI initiatives, such as personal PKI certificate storage and usage.

28. The same functionality that is available via the interactive interfaces will also be available via programmatic access.

29. LDAP access will be provided to Directory data, while ensuring that all modifications made via LDAP are subject to business logic and data validation before being stored in the ID Vault Directory. This will be done to ensure that the data management principals, guidelines, and specifications of the Governance Board are enforced.

30. LDAP access to the Directory will support Kerberos authentication via GSSAPI and Kerberos pass-through via secure simple bind. Clear-text simple bind will be disabled.

31. LDAP access to the Directory will support X.509 certificates-based mutual authentication.

32. The Registry will store all data received from each source, including the Sponsor System, in order to reconcile data changes against other data sources in near real time, 24x7. This facilitates the evaluation of that data without the need to contact the source, thus shielding the MCommunity system from source system outages.

33. Identities created in the Registry will be assigned a system-generated unique identifier.

34. The Registry will not have a dependency on any data source for the naming of the objects it contains.
35. A process will be responsible for assigning unique identifiers (such as UIDNumbers and GIDNumbers) to identities in the Registry. The UIDNumber values will need to be unique, and those assigned to identities with uniqnames need to persist indefinitely.

36. A population process will populate a forward-facing and less restrictive Directory with identity data that has been consolidated to represent the current and authoritative state and that has been subjected to institutional data precedence rules defined by the Governance Board.

37. Population/de-population of Registry Identities into the Directory will be governed by criteria to be set forth by the Governance Board.

38. The ID Vault will perform graceful de-population of identities from the Directory to facilitate service de-provisioning needs.

39. One or more processes will use identity data in the Directory to manage memberships of identities in Institutional Roles in the Directory in near real time as defined by the Governance Board.

40. Sponsorship expirations will be processed by providing appropriate notifications, performing data cleanup, and ensuring de-population from the Directory and the Registry when appropriate.

41. The system will interact with Kerberos to create, disable/delete, and modify Kerberos Principals.

42. The system will provide authorized service providers with elevated access to directory data that is not hampered by white pages privacy settings.

43. The ID Vault will provide the capability to exercise the MAIS Search/Match Bio-demographic data update (SMBIO) process to assign UMIDs for Registry identities when appropriate.

44. The system will represent Directory data using object classes appropriate for the task.

45. Thoroughly documented, consistent, and predictable data-maintenance practices will be implemented.

**Operations Requirements**

The operations requirements focus on the running of the system itself and will be of greatest interest to the MCommunity staff.

46. The ID Vault will use effective replication techniques, including geographic diversity, to provide fault tolerance, fault impact isolation, and load distribution.

47. It will use effective partitioning techniques to facilitate replication and security.

48. It will employ multiple security techniques to strictly enforce limited access to the Registry data to only those users and processes that require access. This will include physical security, network filtering, firewalls, ACLs, replica placement isolation, and so on.

49. We will deploy and customize a solution that meets the needs of the institution while maintaining an appropriate level of supportability by vendors.

50. We will implement and configure logging mechanisms for all system components to allow for troubleshooting system performance, functionality, and integrity.

51. We will implement and configure auditing mechanisms for all appropriate components for the purpose of recording data access and modifications throughout the system. The Governance Board will steer implementation of auditing by determining what is appropriate to audit and to what level of detail, as well as determining the appropriate retention and reporting of this information.

52. We will create and implement effective change-control processes and procedures for appropriate components.

53. We will deploy appropriate backup solutions for data, configuration, processes, and systems.
54. We will develop and test disaster recovery plans and include them in the operational procedures.

**Dependencies**
- The ID Vault is dependent upon host level security, including IP filtering and firewalls, as the first line of defense in the protection of the Registry.

**Questions, Future Enhancements, and Design Considerations**

**Policy Questions**
- The Governance Board will steer implementation of auditing by determining what is appropriate to audit and to what level of detail, as well as determining the appropriate retention and reporting of this information.
- The Governance Board will define the precedence of data from multiple sources, which will be present in the Directory.

**Design Considerations**
- We will work with the alpha testers to determine true needs and business relevance regarding the definition of non-personal entries.

**Future Considerations**
- Individuals could be given the ability to grant and manage granular proxy access to their personal identity data.
- The ID Vault could include an interface for creating and exporting identity data. Examples include ldif, vcard, and so on.