Background
The Enterprise Directory Project team conducted six open focus group sessions and several additional sessions with existing technical teams to gather requirements for a future Enterprise Directory Services. The results of these discussions have been consolidated and summarized and specific requirements identified. These requirements will be used to assess various possible technical solutions and to produce a recommended software platform. In addition, these requirements will assist the project team in identifying a recommended scope of effort for implementation and will constitute much of the business case we will deliver to the executive officers.

Overview
The requirements are written as statements and represent what we heard the campus community express as needed functionality or technical specifications. In addition, to help clarify a specific requirement that may not have a current common definition, we have provided several case scenarios.

Requirements:

1. Provides a common set of institutional roles, well defined and communicated, including a common understanding about how they are managed and the ability to create additional roles that may be defined locally. This includes a mechanism to allow groups to be created based on reusable rules. These roles and groups will serve as the basis for authorization to services by individual units or departments.

2. Provide a mechanism for proxying and delegating authority to others for record management (e.g., Professor Jones gives John Adams authority to proxy her directory entry and to make updates to user-defined fields such as preferred phone number).

3. Provide a mechanism to allow greater granularity to what is published in the directory based on an individual’s preferences. Include explicit information about what the privacy settings will or will not do.

4. Provide multiple layers of security to support those with varied need to know in performing their jobs including separate views for the world, the University community, and individuals.

5. Follow institutional policy on the minimum data to be published for all faculty, staff, students, alumni and other affiliates which conform to all applicable laws (FERPA, FOIA, etc.). Establish thresholds for the maximum amount of information to be included. The Provost’s Privacy Committee will be responsible for establishing these policies and resolving any related issues pertaining to privacy and the directory.

6. Provide a distributed, standardized method for creating identities that is easy to use and allows units to leverage the directory for account provisioning. The process by which identities are created should account for loosely affiliated individuals, such as visiting faculty, campers, etc. It should also enable secure identity creation without the need for a physical presence, and should include the ability to create temporary or reusable entities.

7. The ED must interoperate with the following technologies and systems:
   a. File systems – AFS, NFSv4
   b. Security mechanisms – CoSign, KX.509, Kerberos, RACF
   c. Operating systems – Mac OS X, Linux
   d. Directories – Microsoft Active Directory, Novell eDirectory
8. The ED must incorporate common standards, including those which allow for the use of multimedia and inter-institutional collaboration. A separate set of proposed directory standards is included as an addendum to this document (please see Directory Standards).

9. Provide a flexible set of methods for accessing data within the directory and for adding/updating data. These methods should include well documented application program interfaces (APIs) for multiple platforms, native client access, common file layouts, wizards and other tools. These access methods will provide the ability to integrate the ED with listservers, digital asset management systems (DAMS), directory enabled networking, email, card access systems and keyservers.

10. Provide the ability to extend the directory with local sources of information.

11. Provide a mechanism to directory enable applications and to subscribe to other University directory services.

12. Deliver data attributes that are granular and concise, avoid attributes with multiple pieces of data. Include historical information and last update date and source for each attribute.

13. Provide attributes for:
   a. Student status, level, academic plan, major and registration status
   b. Faculty and staff appointment start and end dates, percent of appointment, and department
   c. Faculty assignments and areas of research
   d. Affiliations (official and non-official), preferred contact method, multiple addresses, distinguished names, phone numbers, phone locations, images, and other multimedia, certificates, and a person’s presence (similar to buddy lists).
   e. Certificates such as KX.509

14. Identify the authoritative sources of data with one definitive source for each attribute. Provide accurate and timely data based on campus needs (e.g., what data should be real-time versus nightly update versus weekly, etc). Include input validation (i.e., edit checks) in user-updatable attributes. Keep user modifiable fields separate from authoritative data.

15. Provide the ability to notify appropriate individuals or groups automatically when data are changed. For example, an automatic notification that a person is no longer affiliated with the University would allow units to close accounts and/or deny access in a timely manner.

16. Reduce the occurrence of duplicate identities.

17. Keep directory entries beyond retirement and graduation. Allow for entries to be deactivated and reactivated.

18. Provide the ability to track non person entries in the directory. Non person accounts could include system related entries (e.g., usenet, xserver, oracle, root, etc) or other types of directory objects (e.g., rooms, hardware, networks, etc.).

19. Create a policy for removal of uniqnames that are no longer used so they may be reassigned. Discontinue the use of SSN in creating identities.

20. Incorporate Internet 2 schemas for voice over IP (VoIP) and GRID computing such as eduPerson, commObject, and posixAccount.
21. By virtue of a user’s directory roles, group memberships, and other attributes, provide information about which services a user has access to.

22. Ability to identify resources and to allow for central management of GRID resources including policy files (who may use this specific resource on the GRID).

23. Provide education and assistance in respect to directory services including how to enable applications to take advantage of them.

24. Thoroughly document the implications of making information in a directory public or private.

25. Publish detailed information about the information available in the directory, including rules and policies that govern it, where it comes from, how it is used, how to update attributes and how specific attributes are linked to authoritative sources.

26. Provide help links to explain common roles and assist with using roles for authorization purposes. Provide a directory wizard to answer common directory related questions.

27. Expand search capabilities by adding the ability to search on new attributes and perform fuzzy searches.

28. Provide a web-based, ubiquitous tool for updating and viewing directory information.

29. Provide a streamlined way for creating accounts for unofficial affiliates such as visiting scholars and people who are not physically present.

30. Provide a one-stop directory shop as opposed to departments having to go to many sources for data.

31. Provide a phonebook style format for people to view an online entry.

32. Provide affiliation specific views of data.

33. Provide an automated method for finding forgotten passwords via email.

34. Provide 24 X 7 availability with full backup and disaster recovery

35. Provide a full test environment for development and the ability to create test accounts in the production environment and to track these accounts over time.

36. Ensure the distinction between individual and group entries are apparent.

37. Provide a name space in which groups can be created and propagated between systems.
Case Scenarios and Glossary:

Authorization:
Authorization is the positive determination by the owner of an information resource that a specific individual may access that information resource, or validation that a positively identified user has the need and the owner's permission to access the resource. The following scenarios identify examples of how a directory assists in authorizing access to services. It should be noted that a directory does not automatically authorize individuals to specific services; the directory provides the necessary data for assisting in determining who may be authorized.

Case scenario 1:
Based on data in MPathways, an individual is assigned one or more roles, such as “registered student” or “full-time staff.” A system administrator in the Office of Development may authorize all “full-time staff” to have read only access to a website with information on the Capital Campaign.

Case scenario 2:
An administrator in Engineering can do an ad hoc inquiry of directory data to find all students registered for ME250 along with all instructors assigned to teach this course for Winter 2004. She adds two additional individuals who are faculty at Wayne State that are invited to audit the class. This administrator then authorizes these individuals to have access to a course tools site and related library materials.

Case scenario 3:
An assistant to a professor creates a group in the directory by adding individual members’ uniqnames to a group entry “friends of Professor Smith.” He uses this group to send out email and to authorize these individuals to access the Professor’s AFS space.

Case scenario 4:
Every semester a set of groups are created to support listservs for student government. These groups are created using basic logic to separate students by class level and then to randomly assign them to equal groups. The logic is written once and stored centrally and can be reapplied every semester to the current population.

Authentication:
Authentication is the process of verifying an identity prior to granting access to a computer system, network or source of online information. For example, user names and passwords are common forms of authentication. At the University of Michigan common forms of authentication include CoSign and Kerberos. An Enterprise Directory service will include an authentication mechanism.

Privacy:
Privacy is the right of an individual to be secure from unauthorized disclosure of information about them. The following scenarios provide examples of how a directory can assist in protecting an individual’s privacy.

Case scenario 1:
James Doe has a directory entry as an alumnus. As an alumnus it is determined by policy that the minimum attributes to be viewable to the authenticated UM community are student name, last degree year, and college attended. In addition to these attributes James chooses to publish his personal website’s URL, his preferred mailing address, and his business address. He chooses to keep his telephone number and email forwarding address private and only viewable to those authorized as having a need to know, several individuals in the Office of Development and his personal assistant. When James binds to the directory for each attribute that he has a publishing choice: to keep entirely private, to publish to the UM authenticated community or to publish to the world.
**Case scenario 2:**
Jean Doe has a directory entry as a UMOL subscriber and former student. She has requested to have her information FERPA protected. The only viewable attribute to the UM community is her uniqname. Only the administrator supporting UMOL may see the remaining directory attributes.

**Case Scenario 3:**
A former KGB agent is a visiting lecturer at the Law School. He needs access to library materials and printing resources at the Law School. The administrator at the Law School establishes a fake identity for the individual using a specific set of attributes for a guest account. The only viewable directory attributes are the guest account uniqname and an affiliation to the Law School as a guest.