**Organizational Need**

In October 2008, UA’s Information Technology Executive Council (ITEC) stated that ease-of-access to resources and information provided by UA is of intrinsic strategic value and must be a primary goal of technology service delivery. Optimum design architecture for authentication, identity management and directory services is key to resource access. This standards document outlines UA’s intentions.

**Terms of Reference**

- **UA Users.** Anyone accessing UA-branded resources, including students, faculty, staff, patrons and other authorized individuals.
- **UA Username.** A standard identified (username) recognized throughout UA.
- **UA Credentials.** The combination of UA Username and a secret password known only to users.
- **Services.** Enterprise applications and major services (e.g., email, storage, domain access, calendaring, UAOnline, Shibboleth, eduroam).
- **Unified Directory.** System-wide implementation of a single-forest Active Directory™ directory service.
- **3rd Party Federation.** A method to secure non-UA application/service access using UA identities.

**Architecture Standard**

- Multiple special purpose or local directories
- Complexity associated with updating and synchronization.
- Multiple Kerberos realms.
- Single directory environment with presence at all university-operated locations.
- Single Kerberos realm with significant improvement in design elegance.
- Shibboleth connection to Unified Directory.
- eDIR’s unique person/contact directory functionality retained as an application.
- Synchronization eliminated reducing complexity and potential fault source.