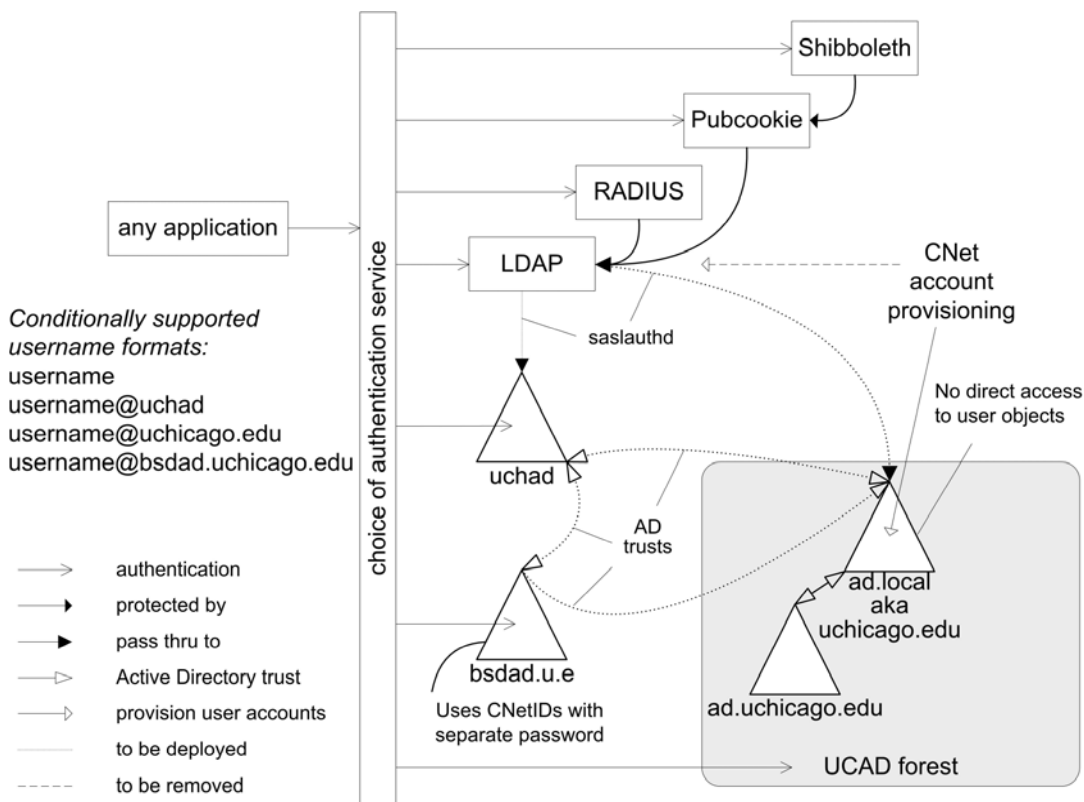


Case Study: University of Chicago Authentication Architecture

University of Chicago (UC) like many organizations, have bought in to the "identity management" paradigm, which presumes the value of using a common credential for the majority of ordinary purposes. For us, that's the CNetID and CNet password. The more applications that use them, the easier things are on end-users and on the IT shops supporting those applications, and the more readily we can adopt or adapt to new functional and operational requirements. And when every U Chicagoan necessarily has a CNetID, we can avoid some of the absurdities that otherwise emerge to work around that deficit.

In addition to these generic benefits, approximately 1/3 of our activity resides in programs and people that straddle the line between UC and UC Hospitals (UCH). Yet those organizations have had independently-managed credentials and authentication systems that burden the line-straddlers, making it harder than necessary to access resources and manage access to resources. We need an infrastructure that enables any IT shop to run any off-the-shelf or custom application to serve people across the union of UCH and UC.

Building on other work to merge CNetIDs with UCH usernames, this infrastructure will allow an application to integrate with any of several different authentication services, each of which routes the authentication back to the appropriate back-end credential store. Passwords of persons managed by UCH will remain in their "uchad" Active Directory domain, and CNet passwords will remain in NSIT's chosen back-end store. That's LDAP plus the root domain of the UC Active Directory forest (UCAD) maintained in synchrony for now, and later we'll eliminate some complexity and keep them just in UCAD.



The diagram shows the various authentication technologies operated by Networking Services and Information Technologies (UC's central IT department), including [LDAP](#), [UCAD](#), [RADIUS](#) (used by some network access services), and the web Single Sign-On systems

Private
13,900 Students
Doctoral Extensive
Tom Barton
May 2006

[Pubcookie](#) and [Shibboleth](#), together with the [Active Directory](#) domains operated by UCH and by the Biological Sciences Division. Trust relationships will be established between those domains and UCAD, enabling AD-integrated applications operated by UCH, the BSD, and NSIT to refer uniformly to people across UCH and UC. NSIT's LDAP service will contain information about where each user's password is stored, enabling applications integrated directly with LDAP, or with any of the other authentication technologies that ultimately depend on LDAP, to likewise support users across the union of UC and UCH.