

Active Directory at the University of Michigan

Data Population and Kerberos Interoperability

MaryBeth Stuenkel

maryb@umich.edu

LAN/NOS/Groupware Services

www.umich.edu/~lannos/win2000

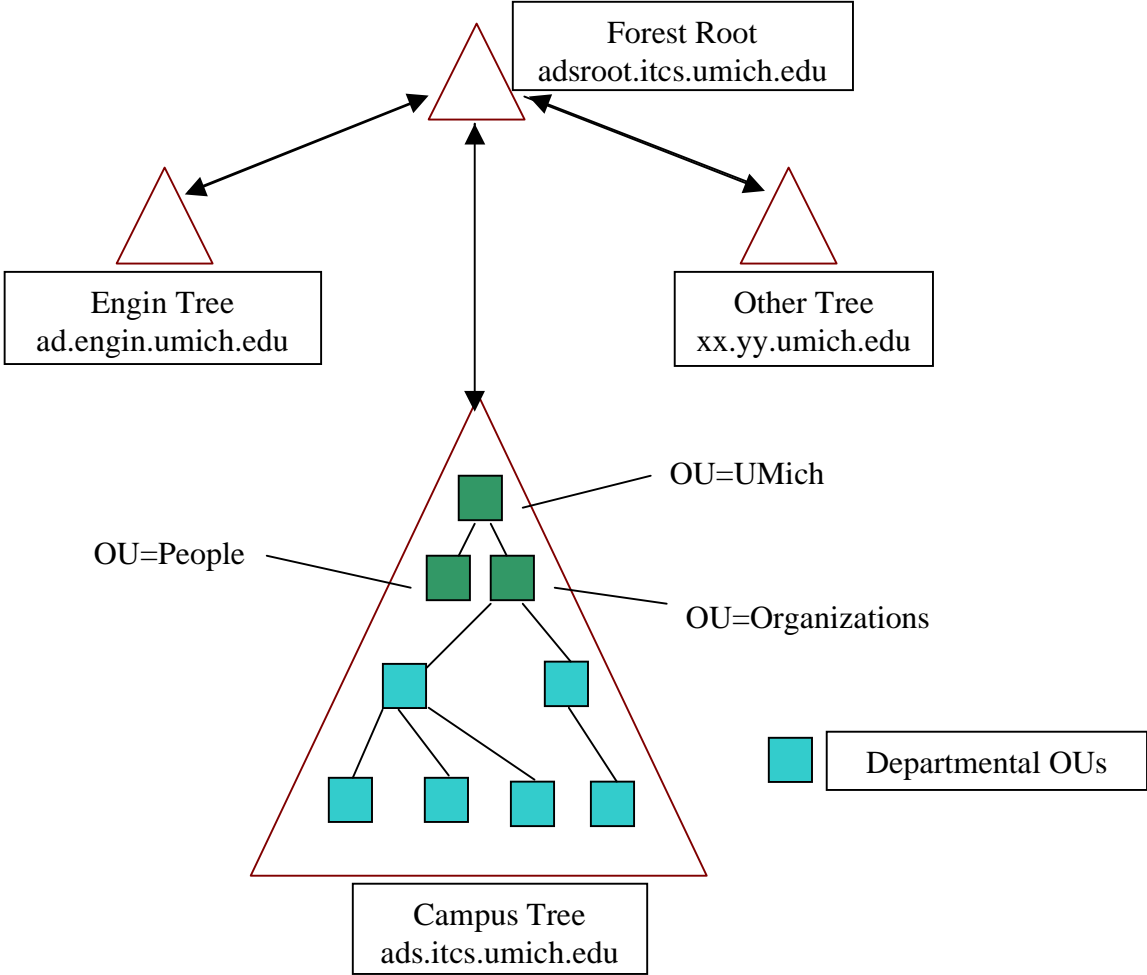
Existing Infrastructure

- Uniqname – every faculty, staff, student assigned a unique 3-8 character identifier
- OpenLDAP enterprise directory
- MIT Kerberos user identity
 - based on uniqname
 - used for directory maintenance, email, IFS filespace
- DNS Structure based upon University Organizational Chart (governed by policy)

W2K Implementation Goals

- Provide an infrastructure that allows for distributed administration within a single forest infrastructure
- Enable transparent user access to resources throughout campus
- Automatically populate AD with data from enterprise directory
- Provide single signon via Kerberos
- Integrate with existing BIND DNS infrastructure

Structure of U-M Active Directory Forest

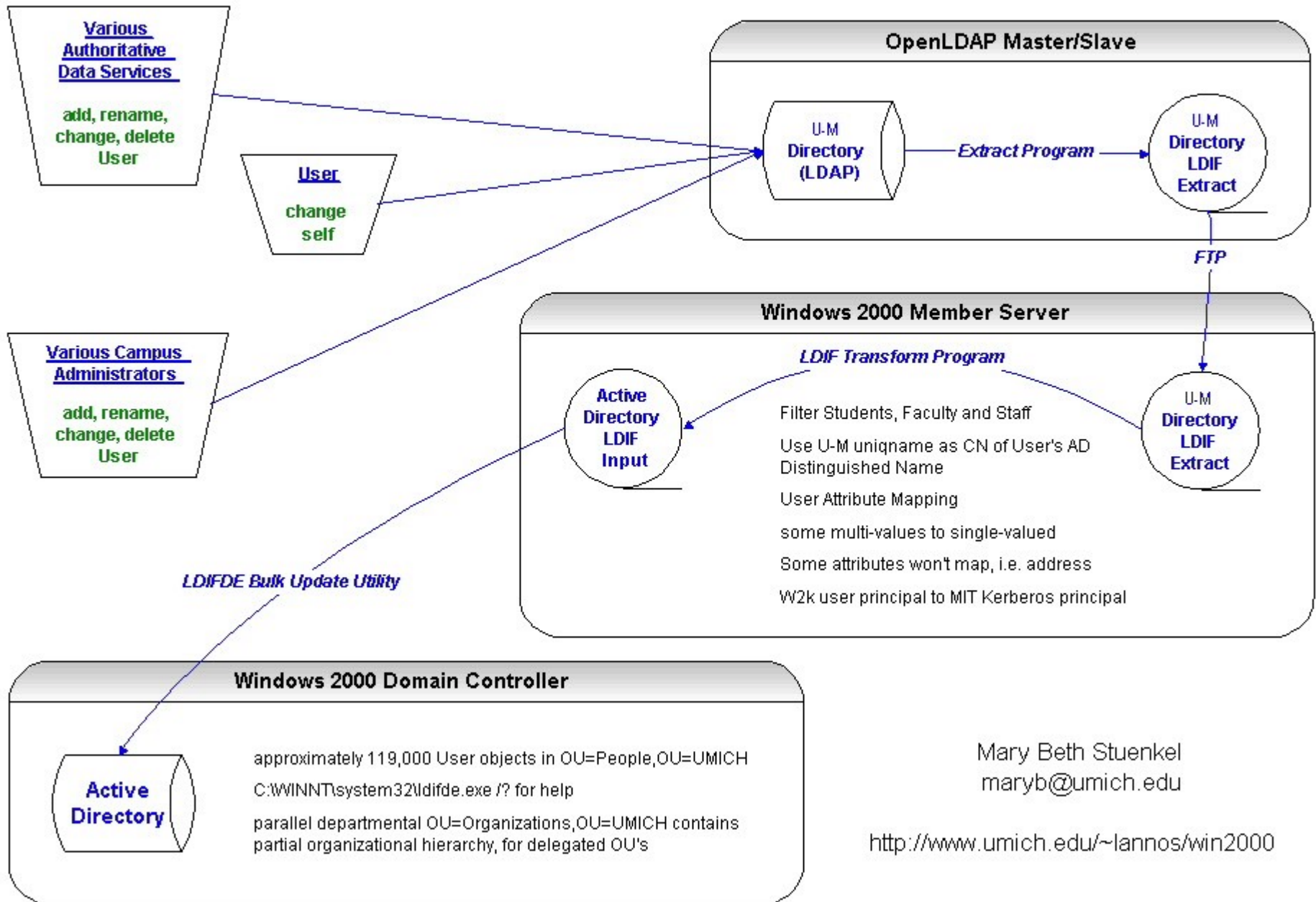


Populating Active Directory

- OpenLDAP directory entries update AD
 - Initial feed/bulk load
 - Automatic updates of changes and new entries
 - Out-of-band updates
- Schema mapping
- Mapping of W2K user principle to MIT realm
- Updates are one-way only, changes made in AD are never passed back to OpenLDAP

Updating AD User Entries from the U-M OpenLDAP Directory

Stage 1: Initial Feed / Bulk Load of Active Directory

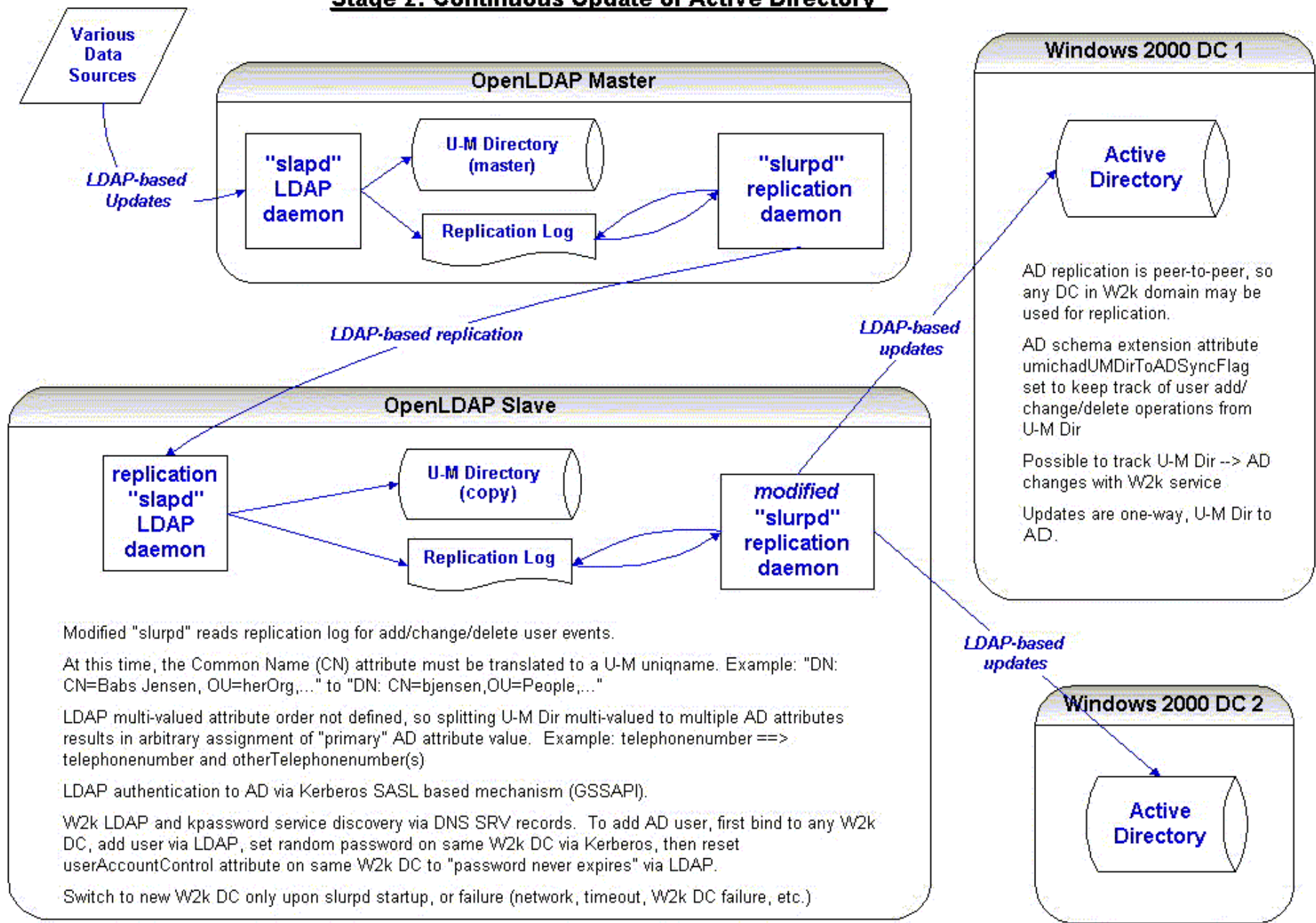


Mary Beth Stuenkel
maryb@umich.edu

<http://www.umich.edu/~lannos/win2000>

Updating AD User Entries from the U-M OpenLDAP Directory

Stage 2: Continuous Update of Active Directory



Active Directory Attribute Mapping from U-M Directory

cn	IDAPDisplayName	Require	isSingle Valued	Mapped from:
	dn	yes	N/A	uid + path (cn=bjensen,ou=people,ou=umich,dc=...)
Common-Name	cn	yes	TRUE	uid
User-Principal-Name	userPrincipalName	yes	TRUE	unique@umich.edu (bjensen@umich.edu)
SAM-Account-Name	sAMAccountName	yes	TRUE	uid (bjensen)
Alt-Security-Identities	altSecurityIdentities		FALSE	<i>Kerberos:uid@umich.edu</i> (Kerberos:bjensen@umich.edu)
Display-Name	displayName		TRUE	cn (Babs Jensen)
Description	Description		FALSE	use AD displayName, derived from cn
Surname	sn		TRUE	sn
Title	title		TRUE	1st value of title
E-mail-Addresses	mail		TRUE	1st value of mail
Other-Mailbox	otherMailbox		FALSE	all mail values after first
Telephone-Number	telephoneNumber		TRUE	1st value of telephonenumber
Phone-Office-Other	otherTelephone		FALSE	2nd to Nth values of telephonenumber
Phone-Home-Primary	homePhone		TRUE	1st value of homephone
Phone-Home-Other	otherHomePhone		FALSE	2nd to Nth values of homephone
Phone-Mobile-Primary	mobile		TRUE	1st value of mobile
Phone-Mobile-Other	otherMobile		FALSE	2nd to Nth values of mobile
Phone-Pager-Primary	pager		TRUE	1st value of pager
Phone-Pager-Other	otherPager		FALSE	2nd to Nth values of pager
Facsimile-Telephone-Number	facsimileTelephoneNumber		TRUE	1st value of facsimiletelephonenumber
Phone-Fax-Other	otherFacsimileTelephoneNumber		FALSE	2nd to Nth values of facsimiletelephonenumber
WWW-Home-Page	wWWHomePage		TRUE	1st value of labeledurl
WWW-Page-Other	url		FALSE	2nd to Nth values of labeledurl
umichad-OU	umichadOU		FALSE	ou
umichad-Role	umichadRole		FALSE	An index "role" attribute; taken from last part of ou values
umichad-No-Batch-Updates	umichadNoBatchUpdates		TRUE	nobatchupdates
umichad-Dir-Sync	umichadUMDirToADSyncFlag		FALSE	2 = user added, 4 = user changed, 8 = delete user, 16 = modrdn
umichad-No-Batch-Updates	umichadNoUMDirUpdates		TRUE	set in Windows 2000

Populating Active Directory

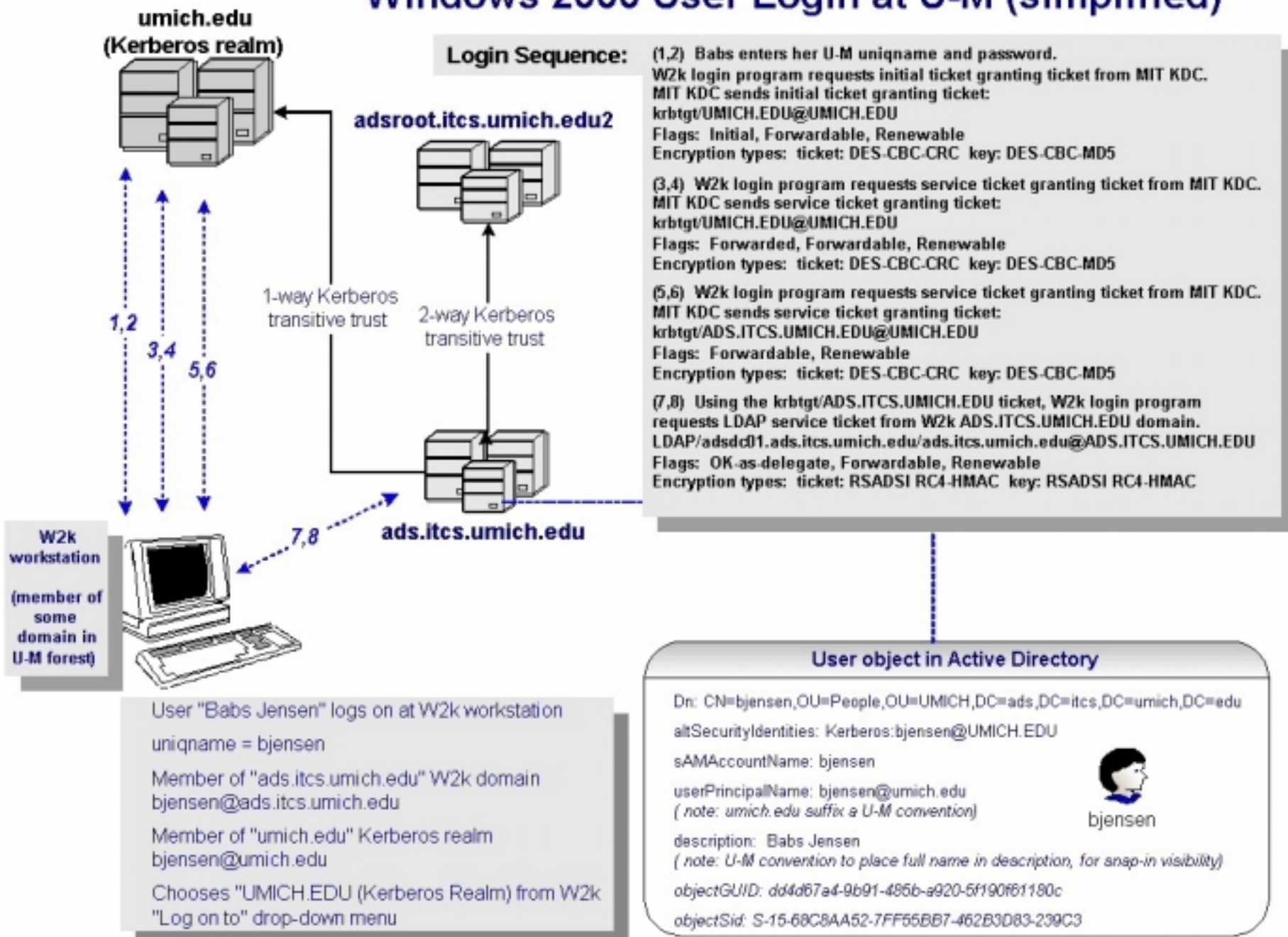
Still left to do:

- Making use of umichadUMDirToADSyncFlag to log/track user add/change/delete operations from OpenLDAP
- Implementing out-of-band updates to OpenLDAP
 - Changes in formats of data feeds
 - Changes to schema of OpenLDAP
- Testing and move to production

Kerberos Interoperability

- Process
 - User presents Kerberos username and password and receives MIT initial ticket granting ticket (TGT)
 - User receives MIT service TGT from MIT KDC
 - User receives ADS service TGT from MIT KDC
 - User uses ADS TGT to request LDAP service ticket from AD KDC
- Details
 - Kerberos v5, release 1.2.1
 - Kerberos passwords NOT synced with AD passwords, AD password not known by user
 - One-way trust only, AD trusts MIT

Windows 2000 User Login at U-M (simplified)



Kerberos Interoperability

Existing challenges

- Applying group policy to users in People OU via loopback processing on computers not working for MIT KDC-authenticated users
- Preventing namespace collisions with current and future unqnames through user objects created by departmental OU admins
- What about non-Kerberos supported clients?

Summary

- Existing infrastructure
 - Both a challenge and an enabler
 - Has provided a rich environment for collaboration
- Automatic data population
 - Coding for initial feed and automatic updates complete
 - Logging changes to AD, coding for out-of-bound updates and more testing to do
- Kerberos interoperability
 - Authentication via MIT KDC working
 - Biggest current issue – loopback processing on group policies applied to computer objects

Credits

- Andrew Wilson
- Dave Detlefs
- Paul Turgyen
- Other UMCE staff
- Technical Lead
- Windows Developer
- Web site Developer
- LDAP Developer
- Kerberos Integration
- DNS Integration
- Directory Integration

w2k.support@umich.edu

www.umich.edu/~lannos/win2000