

November 10, 1999

Ken Klingenstein
University Corporation for Advanced Internet Development
c/o EarlyAdopter@Internet2.edu

Dear Ken,

The University of Michigan (U-M) would like to continue its participation in the Early Harvest initiative as an Early Adopter. We believe that we need to push the middleware envelope as you suggested in a recent e-mail message.

The U-M already provides a substantial middleware infrastructure that is widely used on campus. At the same time it is clear that we have substantial work to do to keep this infrastructure performing well as the number of users and types of use increase. And while we are proud of our existing middleware deployment, it is also clear that we must do more to increase the use of common approaches to middleware across campus. While a widely deployed campus middleware infrastructure will benefit a range of campus activities, we feel that an inter-institutional approach is particularly important to ensure that a critical mass of organizations will be ready to fully participate in Quality of Service and other Internet2 efforts.

Background on the University of Michigan

The University of Michigan is one of the world's premiere research universities. The 52,000 students on the three U-M campuses (Ann Arbor, Dearborn and Flint) come from every state and 115 countries. The Ann Arbor campus, with 24,000 undergraduate, 10,000 graduate and 3,000 professional students and 3,700 regular faculty, offers more than 5,600 undergraduate and graduate courses each term. Students can choose from more than 200 undergraduate majors and 600 degree programs offered by its 19 schools and colleges. U-M research expenditures--more than \$491 million in fiscal year 1998--are the highest among public universities in the United States and second largest of all U.S. universities. The U-M Medical Center, comprised of three hospitals, 30 health centers, and 120 outpatient clinics, is one of the world's largest health care complexes. It treats more than one million patients annually. Additional information is available from the U-M Gateway:

<http://www.umich.edu>

Existing policy infrastructure

All University of Michigan students, faculty and staff have electronic access to the U-M campus network and the Internet including Internet2. This includes on campus access from dedicated network attachments in faculty and staff offices, laboratories, residence halls, family housing, walk-in computing and library sites. Off campus network access is provided using a system that provides local call v.34, v.90 and ISDN access from over 94% of the telephone exchanges in Michigan. An ADSL pilot is underway in Ann Arbor.

Students, faculty and staff on all three U-M campuses are assigned a "unique name" identifier and associated Kerberos password. This identifier is included on U-M ID cards together with the more traditional numeric university ID and social security numbers. Unique names are used to authorize access to many information technology resources on campus including:

- + a general purpose computing or login service;

- + a statistics and computation service;
- + the institutional file system (AFS based);
- + Wolverine Access, a system that allows students to view their student records directly from U-M's student databases and which in the future will allow faculty and staff members to view their employment records;
- + an X.500 directory that provides white page lookups for individuals as well as course e-mail lists and user maintained e-mail groups,
- + various Web based services;
- + campus computing sites;
- + many electronic library resources; and
- + dial-in services.

IMAP, POP and "classic" e-mail access is available to all students, faculty and staff. E-mail forwarding, e-mail groups are managed through the campus X.500 directory service.

U-M Online is a service that provides e-mail and other computing access to alumni, parents, and others affiliated with U-M who are not students, faculty or staff.

For U-M policies on the use of information technology resources check:
<http://www.umich.edu/~policies/>

Existing technical infrastructure

The main components of the existing U-M middleware infrastructure include:

- + A unqname server used for holding and managing unique login identifiers; also used for creating and managing Kerberos passwords. This decentralized U-M-wide system has about 200,000 entries.
- + A Kerberos v5 server used to authenticate ownership of unqname identifiers.
- + A PT server used to check and grant access to various application-specific services, usually based on inclusion in PTS groups which are created and maintained using this server.
- + Kerberos client software to check authentication with Kerberos servers.
- + Integration of client services with desktop applications (using Kerberos v4 protocol at this point).
- + X.500 directory service used for email forwarding, populating UMIAC databases, user created email groups, and white pages lookups; users can update and maintain their own entries.
- + Novell Directory services, used primary for Netware file access and for Groupwise email lookup.
- + Institutional File System (U-M AFS) access is controlled by the unqname-Kerberos-v5-PTS systems described above.
- + Administrative systems ID card database used for maintaining unique non-social-security ID numbers for members of the campus community.
- + Kerberos-based web authentication over SSL used to generate cookies for subsequent authentication.
- + Student systems databases that contain class list information (students, instructors, when and where, course titles)
- + UMIAC is a service that integrates information from unqname, X.500, the ID card database, and the class list database(s) and stores that information in a way that allows faculty to add guests to their courses.

- + CourseTools - UMIAC is used by the CourseTools system to provide an authentication mechanism and to create affiliation groups used to control web access to Lotus Notes/Domino collaboration databases that contain course content and student work.

Issues/topics that we expect our participation in Early Adopters will help us address and/or allow us to contribute to the community:

- + Commercial vs. Open Source solutions for LDAP directory services.
- + Questions related to licensing and cost for LDAP directory services, full-scale PKI solutions and other software.
- + Scaling issues: the current U-M unidname database has little capacity for functional growth and so needs a redesign, many of U-M's current middleware services are scaled for the on-campus population and not for higher volume use by Internet2 QoS, alumni, prospective students, and digital guests.
- + The functionality of the current UMIAC and proposed directory services have significant overlap. We need to understand how best to use limited resources in this area.
- + Future NT2000 service directory services may inter-operate with campus LDAP service.
- + Kerberos authentication for Web access is being built into the M-Pathways (PeopleSoft) student module.
- + KX.509 solution is planned for integration into the next U-M "Blue Disk" CD distribution of client software, but many issues remain to be sorted out.
- + Proper proxy authentication (user to server A, then server A to server B proxy) with KX.509 is being explored.
- + Migration to the Kerberos v5 Server has already happened; most applications still use Kerberos v4 protocol with this server; timeframe for application migration from Kerberos v4 protocol to v5 protocol is being done on a application by application basis.
- + Strategies for more widespread deployment of common middleware.

Resources and commitment

As can be seen from the description of existing policy and technical infrastructure given above there is already widespread use of middleware at U-M. This use involves cooperation from the Ann Arbor, Dearborn and Flint campuses as well as between various academic and administrative departments. The Registrar's Office, University Personnel, the Office of the Chief Information Officer and the Information Technology Division are all actively involved in these efforts.

The Center for Information Technology Integration (CITI) under the direction of Peter Honeyman is available to do research and development in support of U-M's participation in Early Harvest. CITI has been involved in projects related to secure video, encryption and high performance file system (AFS) access. CITI is interested in providing a testbed for development and experimentation with core middleware services including:

- + cross-realm authentication,
- + authentication services, and
- + secure directory services based on LDAP

This testbed would be similar in nature to the Kerberos5 work previously performed at CITI, where we equipped the CITI AFS cell with Kerberos5, integrated it into our campus computing environment, and made it available to other campus organizations for campus-wide deployment.

If appropriate U-M can request the participation of Merit Network staff in the Early Adopter effort. Merit is an independent non-profit corporation that is administratively attached to the U-M. Merit operates the statewide network MichNet, is involved in Quality of Service and

Bandwidth Broker initiatives and in the development of the RADIUS protocol and related authentication, authorization and accounting software.

The Product Development and Deployment (PD&D) group under the direction of Bill Aikman within the Information Technology Division is responsible for the deployment and operation of much of U-M's middleware infrastructure.

With the exception of some additional travel and possible work by CITI, U-M's participation in Early Adopter's will not require a significant commitment of new financial resources over and above what is already planned. Our participation will require changes in priorities with more resources devoted to middleware sooner than would otherwise have been the case.

The development and delivery of information technology resources and systems at U-M is very decentralized. The Information Technology Federation is a common decision making forum that represents all U-M IT providers. It is governed by an Executive Committee that includes representatives of the major U-M IT providers as follows:

- College of Architecture and Urban Planning
- College of Literature Science and the Arts, College of Engineering
- Information Technology Division
- Institute for Social Research
- Medical School
- Office of Provost and Executive VP for Academic Affairs
- Office of the Chief Information Officer
- Office of the Controller
- School of Business Administration
- School of Education
- School of Information
- U-M Hospitals
- U-M Dearborn campus,
- U-M Flint campus
- University Library.

The IT Federation Executive reviewed this letter and endorsed U-M's active participation in the Early Adopters initiative.

Gordon Leacock will take the lead to coordinate U-M's participation in the Early Adopter's effort.

If you have any questions about U-M's middleware efforts or need additional information, please feel free to contact Gordon Leacock (gordonl@umich.edu, 734-763-6184), Bill Aikman (aikmanw@umich.edu, 734-647-9520), Jeff Ogden (jco@umich.edu, 734-936-2025) or myself (jmgriff@umich.edu, 734-763-3528).

Sincerely,

Jose-Marie Griffiths
Chief Information Officer
University of Michigan