SUMMARY OF SURVEY RESULTS

June 2001 Workshop on Directories/Repositories and Certificate Authorities

Prepared for the
National Science Foundation and the Higher Education Community

October 12, 2001

Organizational Committee Representatives:
George F. Covert, Associate Director Computer Center, Iowa State University;
Michael Gettes, Lead Application Systems Integrator, Georgetown University;
Clair W. Goldsmith, Vice President of Information Technology/Chief Information Officer, University of Alabama-Birmingham;
Francis Grewe, Assistant Director, Central Computing Operations, Office of Academic and Distributed Computing Services, University of Minnesota Twin Cities;
Ken Klingenstein, Director of Information Technology Services, University of Colorado at Boulder and Director, Middleware Initiative, UCAID;
R.L. Bob Morgan, Senior Technology Architect, Networks and Distributed Computing, University of Washington;
Jeff Schiller, Network Manager, Massachusetts Institute of Technology;
David Wasley, Assistant to the Associate Vice President for Information Resources and Communications, University of California Office of the President

Available at:
http://www.cren.net

Introduction

The roles of directories/repositories and certificate authorities in supporting the development of an efficient campus IT infrastructure continue to evolve.

To support technology development, technology transfer and outreach, the Advanced Networking Infrastructure and Research Program of the National Science Foundation supported two workshops on these topics to be held in the period between January and September of 2001. The first of these two workshops on Directories/Repositories and Certificate Authorities was held on January 30-31, 2001 in Washington, DC. The second was held June 6-8, 2001 in Minneapolis, Minnesota.

Prior to participating in the June workshop, participants from 13 universities completed a pre-workshop survey on the state of testing and deployment of directories/repositories and certificate authorities on their campuses. The purpose of the survey was to assess the degree to which campuses have begun to plan, discuss, and implement these new technologies. The survey was revised from the earlier January 2001 survey.

This is a report of the survey findings. It provides a snapshot of the “state of campuses” with regard to these new technologies, and helps to project the needs of the IT community in deploying these services.

Executive Summary

The majority of the workshop survey participants reported that they maintain an average of three or more directories on their campus with the majority of the directories being managed by the central Information Technology organization. Most of the respondents reported that they were using LDAP for some of their directory protocol access. Also, many of the institutions also report using implementations of ph, Novell and Active Directory services. Over 90% of respondents stated that there are several working applications linked to these directories. The most commonly cited linked applications are those for providing remote access authentication and authorization, email services and telephone directories.

The majority of the institutions also reported using subscriber agreements that members of the campus community must agree to prior to being able to access and initiate their online email accounts. The process for initially registering campus community members for these services varies. The majority of the institutions reported maintaining systems in which users create and set up their own accounts through an on-line process; other institutions reported having a manual process. Some subscribers require users to "click through" the subscriber agreement, go to URL containing subscriber agreement or read statement of use before permitting account access. Data for this account management is most commonly received from the information databases in Human Resources and the Registrar offices on campus.

Virginia Tech provided a url for its subscriber agreement policy for users. This policy — Acceptable Use Of Information Systems At Virginia Tech — is at http://www.vt.edu/admin/policies/acceptuseguide.html

Ten universities have made first stage plans for the use of digital certificates. The majority of workshop survey participants indicated that their campus has several planned uses for digital certificates. Priority uses are remote access authentication and authorization for campus network services and remote content, email security and server certificate signing for various IT services.

No university completing the survey has implemented a process to issue client certificates. Most universities have no specific date to initially issue client certificates nor do they have an existing subscriber agreement for the use of digital certificates. Only four universities completing the survey have the hardware/software infrastructure in place for a certificate authority. Most universities, even if they do not have an infrastructure for setting up certificate authority, do know which software they want to use. Among the most popular are Apache, ModSSL, and PERL 5+.

Overall, the surveys that were completed indicate that many of the workshop participants are in early stages of planning and attended the workshop for information about how to proceed. According to several participants, the workshop was to be the first, important step in securing this information, as it gave time and resources to begin a detailed discussion on the pros, cons, and standards of practice in these technical areas of implementation.

The biggest short-term issues institutions face over the coming months are developing a plan for PKI implementation and educating users. Securing buy-in for digital certificate technology services from administration and staff is another priority. The long-term issue listed by the majority of the respondents is integrating disparate systems effectively and at the same time leaving management of local systems to those most capable and motivated to solve local problems. Campus/system-wide buy-in for CA service was another strong consideration.

The majority of universities reported that the major barriers that are impeding the implementation of certificate authorities are time, resources and trained staff. Other barriers reported were client software IE/Netscape issues, educating users and initial set up and integration with the LDAP server.

When asked what help CREN or others could provide to help in implementation, most respondents stated that they wanted a set of guidelines to follow or advice from successful institutions to use as guidance. Respondents requested best practices for successful implementation in other universities, estimated costs and problems that may occur, and obtaining buy-in and integration. Also requested were lists of institutions with the products they are using. Workshops and meetings similar to the June workshop were requested that would provide networking with other similar institutions to share experiences and to make valuable contacts.

SUMMARY OF SURVEY RESULTS

Section One: Directories/Repositories

Question 1.1: How many directories and repositories do you have on your campus? Approximately?

The fourteen profiled institutions maintain an average of three repositories or directories. About half of the universities indicated that they have three or four repositories/directories. Two universities indicated that they have more than four repositories or directories.

Note: It is likely that most universities have many more repositories, directories, or data stores that are used to authenticate users and authorize access to specific resources. Some reports suggest that some large organizations may have over 100 data stores used as directories. The goal for launching digital certificate projects would be not identifying all directories, but identifying and managing those directories/repositories/or data stores that will serve as the source for authenticating the users/objects to whom certificates will be used.

Selected Individual Responses:

(1) I've no way to begin to know, must be hundreds. Bear in mind of course for this entire survey. I don't know very much at all about this subject, which is precisely why I am attending this seminar in the first place.

(2) 1 Supplier and 5 replicas

Question 1.2: What types of directory formats are you using on your campus?

LDAP	13
Ph	8
x.500	2
Novell	9
Active Directory	9
Other: Home grown	2
Other: x.400	1
Other: Oracle and DB2	1

Every institution except for one uses LDAP. Most institutions also use ph, Novell, and Active Directory. Most respondents listed 4 directory formats being used on their campus.

Selected Individual Responses:

(1) May be others as well
(2) Novell – decommissioning July 2002
Active Directory – planning stages

Question 1.3: Who manages your directory(ies)?

Dept/College System Administrators	4
Central IT organization	11
Other: Not specified	1

Two institutions have their Department/College System Administrators as well as their Central IT organization managing their directories.

Selected Individual Responses:

(1) Central IT organization – several (Novell, Active Directory) allow limited distributed management

Question 1.4: Do you have any applications linked into your directory/repository?
Question 1.5: If yes, what are the applications?

Only one respondent's institution reported that they do not have applications linked to their directory or repository. One respondent did not specify which applications were linked. The linked applications indicated by the respondents are as follows:

Remote access authentication and authorization for library users	3
Remote access authentication and authorization generally	2
Email services, such as account creation, maintenance and email redirection	8
Telephone directories	5
Account/billing applications	1
Other: Student Employment	1
Other: Access for Blackboard and various administrative applications	1

Email services are the most popular applications linked to institution directories or repositories.

Selected Individual Responses:

(1) Access to campus portal, access to filebox space for personal website creation/maintenance, access to grade reports, access to class drop/add system for class scheduling

Section Two: Campus Environments for Email and Computer Accounts

Question 2.1: What processes are you using for initially registering students, faculty and staff for computer and email accounts?

Every institution except two indicated that they register faculty, staff and students for computer accounts using data from human resources or registrar offices. Automatic generation of accounts is used by nine institutions, while manual request forms are also used by nine institutions. Four universities reported that they have users request their own email accounts through a web application. Most universities have more than one method of registering for email accounts. One institution reported that students swipe their ID cards through readers to create accounts or change passwords.

Question 2.2: How many forms and what type of identification are required for initial activation or input into systems?

Most institutions require at least one form of identification. Five universities reported that they require two forms of ID. The forms of required identification cited include driver's license, birth certificate, PIN and password. One's social security number was also a commonly mentioned requirement. Many universities reported that they require students to show their school ID card as well as their social security number to verify themselves. Some colleges require a legal name, birth date and ID number for initial activation.

Selected Individual Responses:

(1) We are in transition from a completely batch oriented, nightly creation of ids to an on-request web-based system. How a user will "prove" who they are is still being discussed.
(2) One photo ID if no ID has already been created: if an applicant does not have a university ID card, then they also need a departmental letterhead note or something similar.
(3) Mother's maiden name
(4) Require a PIN with an ID card. New students present their university ID and then enter a PIN for activation. Returning student accounts are renewed every quarter upon verification of enrollment

Question 2.3: Do your users sign, read or accept a policy statement on the use of their computer account or e-mail access? Question 2.4: If yes, please indicate.

Only two universities revealed that they do not have a policy statement on the use of their computer accounts. Five universities have two or more methods of accepting the policy statement. Of these five institutions, each of them has a statement of use that refers to a more detailed policy coupled with another form of agreement. The University of Illinois at Urbana-Champaign has a statement that refers to a detailed chart showing which group is allowed access and for how long. See http://www.cio.uiuc.edu/policies.html.

Users "click through" agreement to acknowledge acceptance	4
Users are directed to URL containing subscriber agreement	6
Users read statement of use that refers to a more detailed policy	6
Users read on-line statement and take on-line quiz to ensure reading and understanding of agreement	0

Selected Individual Responses:

(1) Policy statement is available but users are not forced to read or acknowledge it
(2) Url of agreement at Virginia Tech is at
http://www.vt.edu/admin/policies/acceptuseguide.html

Section Three: Campus Environment and Uses of Digital Certificates

Question 3.1: Has your institution made plans for the first uses of digital certificates on campus?
Question 3.2: What are some of your planned first uses for certificates?

Ten universities have made first stage plans for the use of digital certificates. Five institutions identified the use of server certificates as their highest priority. In ranking their order of priorities, remote access authorization for campus network services and secure email also received high priority. Remote access authentication for remote content services, server certificate signing for various IT services and E-commerce were also each ranked as top priority by a university. The table shows the number of instances for each of the projected uses of digital certificates.

Server certificate signing for various IT services	5
Remote access authentication and authorization for campus network services	4
Secure Email	4
Email signing	2
Email encryption	2
Remote access authentication and authorization for remote content services	2
E-commerce/on-line purchasing	2
Trusted access to medical information over the web	0

Selected Individual Response:

(1) We really plan to do all of the above, including medical info, but in our case it will be vet-med info.

Question 3.3: Has your institution implemented a process to initially issue certificates to students, faculty and staff?
Question 3.5: If no, when do you plan on issuing the first certificates in a pilot?

No university has implemented a process to issue client certificates to students, faculty, and staff. Most universities have no specific date established for issuing client certificates. As the responses below indicate, campuses are issuing and using server certificates, but are primarily testing and experimenting with hardware and software. One campus indicated a Fall 2001 beginning.

Selected Individual Responses:

(1) Not sure.
(2) No established date for client certificates. Been issuing server certificates for two + years. Currently our office coordinates server certificates with commercial vendors. We used VeriSign onsite for two years, now switching to Thawte. No other current use of PKI, or active planning yet for client certificates.
(3) We are still testing a variety of vendor products. No date has been set that I am aware of.

(4) Awaiting system wide effort developments
(5) Within the next 6 months, still being designed
(6) Fall 2001 via secure web page
(7) Pilot to start this summer, 2001 with an implementation of VPN for remote access. At this time we will start with the IT-staff and see what works best for us.

Question 3.7: If you have implemented or are planning to implement a registering process, which office(s) within the university will have responsibility for approving the issuing of certificates?

One-half of the universities surveyed had no response to this question. Of the seven total responses, six universities will place responsibility for approving the issuing of certificates within their IT/Technical Services department. One university delegates this process to the registrar's office and human resources.

Question 3.10: Do you have an existing subscriber agreement for the use of digital certificates? Question 3.11: How will you modify it for the use of Digital Certificates?

Of the fourteen responding universities, none replied that they have special agreements for the use of digital certificates. Oklahoma State University, however, said that they would update subscriber agreement annually as appropriate.

Question 3.12: Do you have policies and procedures to protect the private key of your institution's certificate?
Question 3.13: Please check all policies/procedures that apply.

Only two universities have private key policies. One university has a private key stored with multiple physical security safeguards as well as a dual control person access in place to activate private key usage of the institution key.

Section Four: Technical Implementation

Question 4.1: Do you have an infrastructure that you are setting up for your certificate authority?

Four universities surveyed replied that they do have an infrastructure to be used for certificate authority. There are nine universities that have not set up an infrastructure for certificate authority.

The four universities use the following infrastructure (of the given choices):

Separate hardware for certificate authority and registration authority	2
Set up a root CA and subordinate CAs with the root private key stored in hardware and activated when required	2
Use CREN institutional certificate as the higher-level CA service	0
Use Windows 2000/Active Directory on a stand-alone system in a physically secure area	0
Active Directory Service-based with some information registered in SQL server	0

Question 4.3: What is the software you are using, or planning on using, including version number?

Most universities, even if they do not have infrastructure for setting up certificate authority, know which sets of software they want to use. The software mentioned most often was Apache and PERL 5.

IPlanet Certificate Management System 4.2	4
Windows 2000	1
Microsoft SQL server 7.0	0
Open SSC 0.9.6	2
Apache	7
ModSSL	5
PERL5+	5
Windows and Exchange 2000	2

Selected Individual Responses:

(1) We are writing an RFP for this and iPlanet is on the list of vendors, along with Mirapoint and Microsoft.

Question 4.4: What hardware is being used or planned?

Five universities plan to use SUN E250 with Solaris 8. Other specific hardware devices planned to be used by a university are: Netra and 3 SUN E-250 Servers; Dell Power Edge 4400 and 6300 servers; SUN E6500, SUN E450, and Netfinity7100’s; and Sun Fire 3800, Solaris 8. More unspecific responses included a dedicated Linux server and preferably not a Solaris, Microsoft or Linux environment.

Question 4.5: Where and how do you secure your CA server?

Only three of the fourteen respondents answered this question. Each corresponding university plans to use two levels of access. The descriptions are as follows:

(1) Secure room and secure rack
(2) Server will be physically secured in a machine room requiring badge/card access. Server will be further secured by password protection, tripwire/ipfilters/log checker software.
(3) The system will be secured in a highly restricted and protected area managed by the Data Center

Question 4.6: Which office(s) within the university has or will have responsibility for the secure CA environment?

Eight universities will rely on the Information Technology department to secure the CA environment. The Network Services group specifically will be responsible in three universities.

Section Five: General Planning Issues

Question 5.1: What are some of the biggest issues in the short term, in the next four months?

The responses to this question confirmed that most institutions responding to the survey are still in the planning stages for PKI implementations. The responses also confirmed that energy was committed to educating users and securing buy-in about the use of the technology.

Developing a plan for PKI implementation	7
Migrating away from existing directory systems configurations to structuring directory information to prepare for PKI by moving to the use of the LDAP protocol	3
Securing buy-in for digital certificate technology services from administration and staff	5
Educating users	7

Selected Individual Responses:

(1) We are already using LDAP, but we are also in process of decoupling authentication/authorization services from being directly tied to our email system. This will be our first step. As part of this process, PKI/certificate authority will come into play.
(2) Completing system wide efforts

Question 5.2: What are the outstanding issues regarding the CA service that you see in the future?

The responses to this question indicate similar set of issues in getting buy-in, management education and general organizational learning.

Campus/system-wide buy-in for CA service	5
Cost issues	2
Educating Management	2
Integrating disparate systems effectively and at the same time leaving management of local systems to those most capable and motivated to solve local problems	8

Educating the users is also an outstanding issue regarding CA as addressed by one respondent.

Question 5.3: What barriers, if any, are impeding your implementation?

Most universities responded that time and trained resources are some of the barriers to implementing CA.

Selected Individual Responses:

(1) Time from IT Staff to do the technical background work mostly. Although there are many products to choose from, no one vendor/product meets all the needs currently. Integration and implementation issues cannot be solved by management, even though they're the ones who are driving the project.
(2) Knowledge and intern application developer resources
(3) Lack of trained personnel

(4) Time and priorities
(5) Vision and resources
(6) Client software IE/Netscape issues
(7) At this time it is educating the users about the long-term benefits of setting up a PKI. Several colleges/divisions are concerned with the centralization of services – single point of failure.
(8) Initial set up and integration with our LDAP server

Question 5.4: What help can CREN or others provide to help your implementation?

Most respondents want a set of guidelines to follow or advice from successful institutions to use as guidance.

Selected Individual Responses:

(1) Provide best practices or guidelines for implementation with examples of successful implementation in other universities. Estimated costs and/or problems and pitfalls will be helpful.
(2) Get the CREN CA into the browsers (IE/Netscape)
(3) Best practices for obtaining buy-in and integration
(4) Provide Root CA service for Inter Institution collaboration.
(5) Workshops such as this one. Possibly a “roll-your-own PKI kit” for the nervous.
(6) Sharing the experiences of other similar institutions and allowing us to make contacts with one another; publishing lists of institutions and the products they are using.

Appendix A

Workshop Survey Respondents

Name	Title	Institution
Konrad Brandemuhl	Manager, Enterprise Systems Services	Oklahoma State University
William Dougherty	Team Leader, Electronic Communications and Client Tools Team/Information Systems & Computing/Systems Engineering Dept.	Virginia Tech
Michael Grady	Senior Research Programmer/Manager, Software Development Group	University of Illinois at Urbana-Champaign
Norman Grant	Manager, Systems	Western Michigan University
Michael Hodges	Manager, Systems Engineering	University of Hawaii
Tom Kitterman	Specialist, Computer Systems Control	Florida State University
Michael Mays	Enterprise Systems Consultant	Temple University
Randall Moory	IT Policy Analyst	University of California at Davis
Patrick O'Callaghan	Director of Telematics Services	Universidad Simon Bolivar
James Parlette	Systems Developer/Engineer Directory Services Administrator	The Ohio State University
Rick Richmond	Project Coordinator, Technical Support	University of Wisconsin-Eau Claire
Larry Schiebel	Sr. Systems Engineer	University of Wisconsin
Donna Tatro	Manager, Collaboration Services Group	Princeton University (Pilot)
Javier Torner	Information Security Officer	California State Univ. San Bernardino