WAVE1 DIGITAL CERTIFICATES PILOT MEETING

BI-MONTHY CONFERENCE CALL

MAY 22, 2002

Wave1 participants met for their bi-monthly conference call on May 22. Bob Brentrup, from Dartmouth, chaired the meeting. Other participants were Larry Levine from Dartmouth, Susan Minai-Azary , Jeff Schiller and MacKenzie Smith from MIT, Dan Oberst from Princeton, Eric Celeste from the University of Minnesota and Judith Boettcher, Michelle Gildea and Ann Symonds from CREN.

Follow Up From May 1 Meeting

Bob began the meeting with an update from the previous phone conference on May 1. He reminded the group that he had placed the first draft of "Using Web Resources with Personal Certificates" on the web:
http://www.dartmouth.edu/~pkilab/pages/Using_Web_Resources.html
Bob encouraged the group to review the site, if they haven't already and to give him feedback.

After some discussion the group agreed that the audience for Bob's site is most likely the IT staff and not end-users. Bob's work on browser support and other technical issues will be particularly useful for those setting up an infrastructure for digital certificates.

Susan reminded the group that MIT has an end user site that members of the group may want to review before setting up their own end-user educational web sites. The URL for this site is: http://web.mit.edu/is/help/cert/   (There was a typo for this URL in the last set of minutes, so please refer to this URL instead.)

Bob indicated that Dartmouth, and most likely Princeton and The University of Minnesota will set up similar user sites and may wish to collaborate with common templates, etc.   Bob plans to ask someone among Dartmouth's web personnel to begin work on formatting an end user site.

In addition, Judith offered to provide a common link to Wave1 Participants on the CREN web site. Those who wish to share URLs and other information should send this material directly to Ann Symonds (ann.symonds@verizon.net) and she will make sure it becomes incorporated on the CREN site.

Update on MAC OS 10and browsers

Bob has been monitoring developments on Mac OS 10 for support of digital certificates. Apple has announce d operating system level certificate storage support and will be publishing an application programming interface (API) for it. This could be a significant improvement that we hope will speed the addition of support for personal certificates in OS X based web browsers.

Eric added that he used a current release of Mozilla to import a certificate from Netscape.

Campus Progress Since May 1 Meeting

Dartmouth: Bob has faxed his application to CREN to get the CREN Root signed. He has also met with the academic computing group to introduce them to the idea of digital certificates and will be meeting soon with the library to get them onboard, as well. Bob will ask the library to identify and select the target audience for the pilot. He plans to begin with staff users and then migrate to faculty.

The Dartmouth team has been working with the iPlanet CMS software to develop an online campus PKI registration system. They have learned CMS was designed to use the UNIX-user id field in the LDAP directory by default. Since Dartmouth had not populated this field in their production LDAP system, alternatives were being investigated. Dartmouth has also been testing plans for recovering the system in the event of hardware failure and discovered that it is essential to have the hostname of the new machine match the old one. Moving to a new IP address proved to be more complicated than expected.

University of Minnesota: Eric delivered an update he received from Frank a few days ago. Frank has issued certificates to the Office of Information Technology. Eric plans to be trying them this week. Because of other priorities, Frank will not be releasing certificates to a wider audience until July.

In addition, Frank has set up the system so that users will have a choice to use a password or digital certificate to access campus resources requiring authentication. Judith had the opportunity to observe Frank demonstrate this capability at the Internet2 meeting.

Princeton: Dan is planning to arrange the signing ceremony for the July/August time frame. The main issue for Princeton continues to be the lack of urgency . Without a strong client need it remains hard for Dan to push the project ahead of others.

Dan's comments led to a brief discussion about campus applications. Bob indicated that Dartmouth is planning to replace Kerberos at the library with digital certificates stored on hard disks and then work on providing a mobile ability. Dan indicated that he is researching the Rainbow I Key device. Bob said the Dartmouth team had gotten one other brand of device and was looking at others. Dan mentioned that another possible application would be to have digital signing with Acrobat. For instance, an expense report could be signed using a digital certificate.

MIT: Jeff updated the group on MIT's status. MIT has many applications for and users of digital certificates. All of the students, half the staff and about a third of the faculty have been issued digital certificates. Digital certificates are a regular part of campus activity. The current set of certificates will expire on July 31. Jeff plans to have the next generation signed by the CREN CA and ready by June 15.

Susan introduced MacKenzie Smith , who is affiliated with the MIT library. She will be identifying members for the Wave1 test pilot towards the end of July.

CREN: Judith asked the group if they had heard of the Department of Education's suggestions that universities each be assigned a unique institutional identifying number for their digital certificates. If this is so, it might be good to identify a place within the certificate profile in which this unique number might be included. This is a question that is being brought to the TAG group. Bob agreed it is be important to monitor these developments, perhaps during the TAG calls.

Update On Collaborative Efforts

Since the last conference call, the group agreed it won't be necessary to ask JSTOR to recognize test certificates from CREN.

Dan offered to share the material Princeton is generating to describe the necessary steps for the signing ceremony. This is currently under development within Dan's team.

Next Steps

Bob mentioned his desire to become more familiar with Shibboleth and its related work. Judith said it is her impression that Shibboleth is being developed primarily as a way to provide anonymous authorization for secure access to external resources , but may also evolve to other authorization purposes. The group will continue to monitor Shibboleth.

Action Items

Dartmouth, Princeton and the University of Minnesota will collaborate on materials for user education.

Michelle will develop a section on the CREN web site for Wave1 links and resource material. Campuses should email this material directly to Ann, who will coordinate with Michelle.

The next conference call is scheduled for June 19 at 11 A.M Eastern Time.