WAVE1 DIGITAL CERTIICATES PILOT MEETING

BI-MONTHLY CONFERENCE CALL

JUNE 19, 2002

Wave1 participants met for their bi-monthly conference call on June 19th. Present were the Chair, Bob Brentrup and Larry Levine from Dartmouth, Susan Minai-Azary, Jeff Schiller and MacKenzie Smith from MIT, John Douglas from Georgia Tech, Eric Celeste from the University of Minnesota, Dan Oberst from Princeton and Judith Boettcher, Michelle Gildea and Ann Symonds from CREN.

REVIEW OF MINUTES

The group approved the set of minutes from the May 22 conference call. These and other past minutes are now posted on the draft CREN site for the Wave One documents. The URL for that site is: http://www.cren.net/crenca/wave1/index.html This is a draft temporary page, and a newer page is in the works.
Judith encouraged everyone to send Ann materials and links they would like to share on that site. Michelle will post them.

CAMPUS UPDATES

DARTMOUTH: Bob is continuing to develop the materials to post on the user web site. He will be meeting with the Dartmouth web consultants to further this along. In addition, Bob has about 10 users downloading and testing personal certificates on local web sites They are working to recruit 10-20 more at the library.

Developmentally, Dartmouth is exploring several concepts. Staff are testing an online CA enrollment program in which a user will be able to log onto the Dartmouth name directory to get a personal certificate. Dartmouth also has plans to modify their existing Oracle database applications to accept client PKI certificates as well as Kerberos tickets.

Bob's team continues to check other browsers for compatibility with digital certificates. They tried some browsers running on Linux that were not able to acquire a certificate from the iPlanet enrollment system. The Mozilla 1.0 browser worked fine and could export the certificate which could be imported into the other browsers however. The browsers they tested were Galeon 1.2.x and Opera 6.0.1. They have not yet found a browser that supports dual key pair generation.

UNIVERSITY OF MINNESOTA: Eric reports no new developments regarding the Wave1 pilot implementation. As planned, Frank intends to roll out the pilot in July.

Currently, Frank's staff is testing and using certificates. Eric hasn't had an opportunity to be part of this test, but he has used the CREN test certificates and MIT certificates. Frank is hoping to have the librarians working with JSTOR soon.

MIT: All campus certificates are due to expire on July 31. Jeff had hoped to covert campus servers to accept CREN certificates in time for next year's issuance of certificates. Having run out of time, he has developed a work-around with both the MIT root and CREN root in the server that will allow MIT servers to also accept CREN certificates. His long run goal is to configure his servers to accept only CREN certificates.

For the first time, MIT will be issuing certificates to incoming freshman prior to their arrival on campus. This will give new students remote access to the housing lottery and other resources they may need prior to matriculation. However, for security purposes, MIT doesn't want parents or other individuals to have continuing access to the freshman's certificate from a remote location after the student arrives on campus. Thus, Jeff and his staff have developed a work around that causes all off-site freshman certificates to expire on August 31. Freshmen will be issued new certificates for campus-use only after that time.

MIT's goal for the CREN pilot is to have the administrative staff using CREN-signed certificates by July 15. The selected staff will then have both an MIT and CREN certificate. In order to avoid confusion over selecting the appropriate certificate each time the user accesses a new site, MIT is developing an automatic selection process whereby the computer is set to select the correct certificate.

Jeff's presentation of his plan led to a more general discussion of the difficulties posed using certificates with IE. Jeff suggested that campuses might use their collective clout to urge Microsoft to correct these problems and fully support digital certificates. Susan offered to bring up this topic as an agenda item for the September CSG meeting. She sent an email to Paul Hill asking him to approach Microsoft to request that representatives from both the MAC and PC IE groups be at the meeting to discuss Microsoft's plans for support of digital certificates with IE.

PRINCETON: Dan reports that Princeton is moving steadily, but slowly, towards pilot implementation. Dan has met with the new general counsel and has had positive discussions about PKI on campus. Friday, July 26, is Dan's target date for signing the CREN root. He intends to videotape and possibly web cast the ceremony.

An impending reorganization in the IT group could be positive news for Princeton's implementation of the Wave1 pilot. The anticipated staff changes may free up resources to focus on the pilot.

GEORGIA TECH: John continues to work on the Papyrus software that he is developing for the CREN test. He is working on version 4 and anticipates that he will release version 5 to the public. He has also been familiarizing himself with IE certificate

generation and will have a functioning CA in the next week. By then, John will be ready to work with Spencer to interface with JSTOR applications.

OTHER DEVELOPMENTS

DEPARMENT OF EDUCATION: The group revisited the discussion concerning the Department of Education's recommendations to place a single unique identifying number on campus certificates. Jeff expressed his worry that multiple organizations and institutions may later also demand unique identifying numbers that could lead to an unmanageable list of unique numbers on each certificate. Jeff strongly reiterated the principle of keeping the certificate simple and uncluttered and focused on identity.

BROWSERS: Bob reports that the Netscape 7 release is now available. Microsoft has released a 5.1 update of Internet Explorer for the Mac, but it still has no support for client certificates.

ACTION ITEMS

WAVE1 WEB SITE: Please send any material or updates for the Wave I pilot web site to Ann. She and Michelle will incorporate them into the site. The URL is: http://www.cren.net/crenca/wave1/index/html

NEXT MEETING: Ann will coordinate with Spencer and the group to set a mutually convenient time to reconvene in mid July. The purpose of that meeting will be to make final preparations for JSTOR access by the pilot groups.