WAVE 1 DIGITAL CERTIFICATES PILOT MEETING

CONFERENCE CALL

JULY 22, 2002

Wave 1 participants met for their monthly update on July 22. Those able to attend included the Chair, Bob Brentrup from Dartmouth, Susan Minai-Azary, Nina Davis-Millis and Jeff Schiller from MIT, Eric Celeste and Frank Grewe from the University of Minnesota, Spencer Thomas from JSTOR and Judith Boettcher and Ann Symonds from CREN. Nina Davis-Millis is replacing Mackenzie Smith as the representative form the MIT library. Her title is Head of Systems and Technology Services. Eric Norman from the University of Wisconsin joined the discussion also to learn more about the Wave 1 project.

REVIEW OF MINUTES

The group approved the minutes from the June 19 conference call. These are posted on the CREN Wave 1 site along with minutes of past meetings. The URL for the site is: http://www.cren.net/crenca/wave1/index.html. This site is being updated constantly and is open for review and additions by all Wave 1 participants. Those who wish to suggest material for the site can post the material to the list or send to Ann who will coordinate with Michelle.

CAMPUS UPDATES

DARTMOUTH: Bob reports that he and his staff are making considerable progress towards the pilot start up. He met with the group from the library and they have selected 12 members of their staff to pilot JSTOR using certificates for authentication. The 12 individuals are regular JSTOR users, so that they will be continually accessing and testing the process. Other Dartmouth JSTOR users will continue to access JSTOR as they have in the past without certificates. The separate URL for the 12 users (and all Wave 1 pilot users) is: https://logon.jstor.org/logon/remote

Before Dartmouth can begin issuing personal certificates to the pilot users, they need to get their CREN signed certificate, which is in process. Once the pilot users get a certificate they will need to develop the habit of remembering the password for their browser's key store. There is no central storage of these "certificate" passwords, as there is with mail accounts. So if the user forgets their password he/she will simply request and be issued another certificate. One difficulty of the current deployment from Dartmouth's perspective is the limited mobility of the machine-stored certificate, since local users are used to library access from public machines. The pilot users will only be

able to access JSTOR using digital certificates from the one machine and browser on which they register. Pilot users will be able to get an additional certificate for a home machine. If they are using a browser that supports it, the same key-pair (and certificate) could be exported and imported on a home machine.

In addition, Dartmouth is converting some Kerberos applications over to be authenticated using Dartmouth issued certificates, from a CA signed by CREN. The first set of applications to be converted are administrative applications written using Oracle. The first application to be made available for production use will be the Banner Student Information System.

UNIVERSITY OF MINNESOTA: Frank reports that he has given 25 people permission to issue themselves digital certificates. He suspects that about half of these 25 have issued themselves at least one certificate, to date. All 25 are OTI employees in the CIO group.

Frank is waiting for their CREN-signed institutional certificate to be signed before he can go ahead with the pilot. He and Jeff need to exchange fingerprints and then Frank needs to send his CSR to Jeff.

Frank lent some observations about browser support for digital certificates. He reiterated what others have observed, that those using IE on MAC won't be supported. These users will need to switch browsers if they want to use client certificates on their machines. He has also observed that Netscape 6.2 under Windows XP won't allow installation of digital certificates. However, Frank has been able to download the CREN root on this browser/op system combination.

Frank has been testing various browsers for user friendliness. He has noticed that Opera and IE use default methods to take the user through the necessary steps. Netscape and Mozilla, however, require the user to go back and make choices in order to work through the program. In order to simplify this process for the user, Frank has found it is easier to first download the CREN root into the browser and then proceed through the list of choices. This avoids a doubling back for editorial changes.

UNIVERSITY OF WISCONSIN: Eric Norman joined the conference call this time to learn more about the Wave 1 project. Although he isn't currently a participant, he had questions for the group.

Eric wondered how campuses will prevent students who leave school before their certificate expires from accessing JSTOR and other campus resources. Spencer indicated that in his opinion, the risk of any widespread abuse is small during the pilot. Once more users begin to access JSTOR using digital certificates, JSTOR may consider making programming changes. In addition, JSTOR will ask campuses to monitor, identify and reprimand users who are violating the terms and conditions of the JSTOR agreement.

MIT: There is no new change in MIT status from the last meeting.

PRINCETON: The key generation ceremony will take place Friday, July 26.

UPCOMING CSG MEETING

On the last conference call, members suggested approaching Microsoft at the upcoming CSG meeting to discuss the difficulties using digital certificates with IE. Susan asked Paul Hill about this, but he indicated that the people from Microsoft coming to the CSG meeting aren't the same ones who would handle the groups' concerns. Eric Celeste suggested we might make the same request for a forum at the Educause meeting, but Judith indicated that most of the Microsoft employees at that meeting tend to be from marketing. Judith offered to send an additional email to Paul expressing her concerns about IE and the need to get Microsoft's attention and support for this.

REVIEW OF WAVE 1 WEB SITE

Bob asked the group to make comments on the evolving Wave 1 website. Many hadn't had a chance to review the site recently. Bob encouraged the group to go to: http://www.cren.net/crenca/wave1/index.html and send any comments or suggestions to Ann.

Bob observed that the first time visitor to the site might find it difficult to easily access background information on the pilot. He suggested that Michelle provide a quick link on the first page for immediate access to a brief summary.

REVIEW OF 12-STEP SUMMARY

Judith asked the group to review the 12-step program for getting started with digital certificates. This was put together at the start of the pilot and she was looking for participant comments on its usefulness and accuracy before she considers posting it on the Wave 1 web site. The group agreed a few modifications would make the document stronger. In particular, many feel the listing of 12 sequential steps makes it appear that each item has to be completed before beginning the next. Actually, many of these steps overlap and occur simultaneously. Eric Celeste suggested we simply indicate that the steps overlap in an introductory sentence. The other option is to make a flow chart or other document that is more visually explanatory.

Bob recommends we add an additional section to the list prior to setting up the campus CA. This should be called, "getting ready for setting up a campus CA." This would include a period for hardware/software review and analysis. The group also suggested it be made clear that campuses need to interact with the directory early in the process, rather than later. Finally, Susan questioned if digital certificates are, in fact, placed in the repository.

As a related aside, Jeff, mentioned that activities reported at the IETF July meeting suggested that PKI may be evolving such that it might be incompatible with the current LDAP standards.

GETTING STARTED WITH JSTOR

Before campuses can access JSTOR for the pilot, they will need to send Spencer a signed certificate in PEM or DER format.

Spencer hasn't had a chance to change the code for the Wave 1 pilot. JSTOR will do another code release in August and he will incorporate a user-friendly URL at that time. For any users who want to access before then, they should use the following URL: https://logon.jstor.org/logon/remote

During the pilot period, Spencer suggests that any questions regarding JSTOR and the pilot should be directed to him. He prefers this rather than to have the "help" desk involved in the pilot.

ACTION ITEMS

WAVE 1 WEB SITE: Please take a minute to review the evolving Wave 1 pilot web site and send comments and additions to Ann. The URL is: http://www.cren.net/crenca/wave1/index/html

NEXT MEETING: The group proposed Wednesday, August 28 at 11 A.M. Eastern Time for the next conference call. Ann will poll the group. If this date doesn't work for the majority, she will identify another that does.