WAVE1 DIGITAL CERTIFICATES PILOT MEETING

BI-MONTHLY CONFERENCE CALL

MAY 1, 2002

The first bi-monthly conference call for the support for the Wave1 Pilot met by phone on May 1, 2002 at 11 A.M. Eastern Time.

Call participants included: Larry Levine and Bob Brentrup from Dartmouth, Eric Celeste from UMN Dan Oberst from Princeton, John Douglass from Georgia Tech, Ed Krol from the University of Illinois, Spencer Thomas from JSTOR and Judith Boettcher, Michelle Gildea and Ann Symonds from CREN.

Bob Brentrup has agreed to chair this group with Ann serving as meeting recorder and general communications coordinator for the group.

The group then turned its attention to user education, which was the topic for the first meeting. The group addressed four sub-topics on user education:

- Browser Support
- Email clients that support S/MIME
- Group collaboration of information
- Next Steps

Browser Support

Bob initiated the discussion by sharing the research Dartmouth has completed-to-date on browser support for personal digital certificates. His group has researched Mozilla, Netscape versions 4.7.X and 6.X on Windows and Mac, Internet Explorer 5.5 and 6 on Windows, OmniWeb and Opera on Linux. Dartmouth has found that Netscape and IE work with personal certificates on Windows, but only Netscape supports client certificates on Mac. Mozilla works well too. Eric added that the Chimera client also supported personal certificates. The Dartmouth PKI Lab is documenting this information on a web page. This information can be found at: http://www.dartmouth.edu/~pkilab/.

Spencer noted that he has used Mozilla and is able to load the CREN certificate on to it. He also shared that he has an "executive" summary and more detailed tabulations summarizing the browser hits on JSTOR during the month of April. After the meeting Ann forwarded the summary to all members of the pilot group. Spencer offered to share the 1.7mb tabulation with anyone wanting greater detail. He can be reached at: spencer@umich.edu.

Email Clients That Support S/MIME

Bob then shared information about Dartmouth's research on email clients that support S/MIME. They have found that Outlook and Outlook Express (release 5 and later) support SMIME mail on Windows. EXMH and Mutt support S/MIME on Linux. Entrust

works with Eudora and Outlook on Windows. S/MIME isn't supported on the Mac by either Entourage or Outlook Express. Netscape works on the Mac and the latest Mozilla includes S/MIME support but there were some bugs in the 0.9.9 release. Bob mentioned that OpenSSL is included in Mac OS 10 and there is hope that new Mac applications will support S/MIME. Details regarding Dartmouth's research on S/MIME clients can be found at http://www.dartmouth.edu/~pkilab/pages/Using_SMIME_e-mail.html.

Group Collaboration of Information

The group agreed it would be useful to share information on user education. Bob has posted some quick start documentation for S/MIME on the PKI Lab site and is working on similar documents for Client side authentication with PKI certificates. Eric mentioned that MIT has extensive user education material and pointed the group to the web site: http://web/mit.edu/is/help/cert/

Bob asked if anyone was interested in collaborating on writing additional user education materials. Members agreed this would make sense as each institution reached that stage. So far, MIT and Dartmouth have begun writing material. Michelle offered to provide links back to the CREN web site to use as a clearinghouse for information shared by the group, and to start building a resource for user education and support.

Bob asked Spencer to inform the group about logistics of gaining access to JSTOR. Spencer said that the JSTOR server will accept certificates signed by the CREN CA Root that expires in 2007. The JSTOR server needs to receive a valid chain of certificates to the CREN CA or the VeriSign CA. Each campus needs to send to Spencer the issuer name for their campus CA to include in JSTOR's authorization tables. (A certificate issued from the campus CA contains the needed information.)

When Spencer was asked if JSTOR could accept certs from the CREN Test CA, he was unsure as to whether we would want to do that. If we did want to do that, Spencer said he would have to do the following:

- Set up a "demo site" within JSTOR to which all users with certs signed by the Test CA would be authenticated. Such a site would have limited content and a limited lifetime, and would serve solely as a demonstration of certificate-based access to JSTOR.
- Modify our certificate authentication code to be able to pull the user's email address from the Subject field of the certificate signed by the Test CA, and to then map that email address to the user's JSTOR site name. This additional code development would have to be scheduled within our release cycle, and could not be in place any earlier than the middle of June.

Not certain that we are all that interested in doing this. Let's check at the next meeting.

Next Steps

Bob said that Dartmouth plans to soon give documentation to the library so they can begin to consider their browser choices and prepare for using personal digital certificates. He also wants to train some of the Dartmouth Help Desk staff to use digital certificates and then have those individuals serve as contacts for trouble-shooting during the pilot period.

Bob said that Dartmouth is testing an iPlanet Certificate Management system which they planned to have CREN sign for the test. Dartmouth wasn't sure if the iPlanet CA needed to be regenerated to have CREN sign it or if a cross certification with CREN would work and was researching an answer. Dartmouth has a self signed Entrust CA in production use which would be difficult to regenerate in order to have CREN include it in a hierarchy if cross certification isn't possible.

Next Meeting

The group agreed to reconvene by phone on Wednesday, May 22 at 11 A.M. Eastern Time. The group hopes to meet every two weeks from there on out. Bob suggested each member spend some time between now and then reviewing the material highlighted on the web. The next meeting will be a continuation of the discussions begun at this meeting.