

**Federal PKI Steering Committee Meeting**  
**November 15, 2002**

Federal PKI Steering Committee (FPKISC) Status:

Four federal agencies have cross-certified with the FBCA: NASA, DOD, Treasury and USDA/NFC.

We're working on Cross Certification Methodology and Criteria documentation that can be used as a how-to and what-to for cross certification with the FBCA. The next version of these documents will be in the January 2003 timeframe.

If your agency has received monies from the FPKISC in the past, you'll be receiving a letter requesting your current status.

A teleconference has been scheduled with the Government of Canada on November 22<sup>nd</sup>. Key personnel from both countries will be identified and introduced in this opening discussion in the process of cross certification between the FBCA and the Government of Canada's CA.

We've performed a preliminary mapping exercise between the FBCA CP and the Government of Canada's CP. There are several issues already identified for the upcoming discussions.

In order to apply for cross certification with the FBCA, an entity must have an operational PKI (it can be a managed service PKI), a CP, a CPS and a compliance audit report.

We've started mapping the VeriSign class 2 managed service policy to the FBCA CP.

We're happy to announce that we've completed technical interoperability testing with VeriSign and that the VeriSign CA is technically interoperable with the prototype FBCA. You'll find a notice concerning this on the FBCA web site.

The Federal CIO Council has been reorganized. The Security Committee was retired. The Enterprise Interoperability and Emerging Information Technologies Committee (EIEITC) was reorganized into the Architecture and Infrastructure Committee. The Architecture and Infrastructure Committee now has three subcommittees. The FPKISC falls under the Leveraging Technology Subcommittee as an Affinity Group.

The Architecture and Infrastructure Committee wants to sponsor a listing of products that federal agencies have used, tested and found helpful.

The Department of Energy representative to the FPKISC is going to brief the FPKISC on the specifics of their document digital signature application. It provides the capability for a user to verify the legitimacy of a document by validating the digital signature using an

Entrust plug-in to Adobe. Energy has purchased a government-wide site license, which will allow any Federal entity to take advantage of the plug-in for their own purposes. There are plans to have the CIO.GOV web site host this and other government-wide plug-in downloads.

Judy Spencer participated at the North American PKI Forum in Dallas, Texas the week of November 4th thru 8th. The North American PKI Forum has joined OASIS and is now considered a membership service under OASIS.

The FPKISC and NIST are going to sponsor a 2-day Federal PKI Deployment Workshop at a major hotel in the DC metro area during the week of February 3<sup>rd</sup> thru 7<sup>th</sup> or February 10<sup>th</sup> thru 14<sup>th</sup> 2003. We haven't decided on an agenda, however, we are encouraging interoperability with the FBCA. Part of the workshop will be about application enablement. Vendors as well as federal agencies will be allowed to exhibit their products and services. We'll advertise via blanket e-mails to federal agencies, IA Digest, Federal Computer Week, Government Computer News and invitations to CIOs. We're planning for approximately 250 attendees.

Judy Spencer distributed to the FPKISC the 2003 Application for FPKISC Funding. We have \$850,000 earmarked for federal agency funding. We'll post this document as well as a deadline date to apply for funding to the FPKISC web site next week. FPKISC funding in FY 2003 is reserved for federal agencies that are developing applications that are PKI enabled, FBCA aware (can process or interpret path validation), and are reusable.

There has been a proposal from at least one new federal agency CIO to create a hierarchical Federal root and require all Federal entities to align underneath it, for the purpose of issuing a standard PKI credential to all Federal employees. The FPKISC is going to respond to this proposal with the assertion that the FBCA could serve a dual function, both as a root that signs your CA for entities that don't want to write a CP and as a Bridge for entities that want to interoperate or cross certify. Judy Spencer and Bill Burr will be drafting a paper on this proposal for discussion at the next FPKISC meeting.

#### Access Certificates for Electronic Services (ACES) Status:

The following federal agencies are now using ACES certificates: State Department, CMS and the Department of Commerce for Exports. We've been having preliminary discussions on modifying the business model. We're also going to update the ACES CP to be RFC 2527 compliant.

#### Next FPKISC Meeting:

The next FPKISC meeting is scheduled for December 11<sup>th</sup> at 9:30 a.m. in the GSA, Central Office conference room # 5141B.

Federal agencies are welcome to send a federal government employee to participate in these meetings. However, government contractors are not permitted to attend these meetings.

**Attendees:**

Judith Spencer, FPKISC  
Brant G. Petrick, FPKISC  
Paul D. Grant, DoD  
Lewis Baskerville, SBA  
Gene McDowell, NOAA  
Marty Burkhouse, DOJ  
Andy Boots, ED  
Bill Burr, NIST  
Kathy Sharp, USDA/NFC  
Steve Duncan, GSA  
John Cornell, GSA  
Dan Maloney, VA