Federal Public Key Infrastructure Steering Committee
February 16, 2001

The CIO Council has posted the FBCA CP to its web site (www.cio.gov) inviting public comment. The CP had previously been distributed to the CIO Council for comment. Judy has asked Lee Holcom, Chair, EIEITC, to close the comment period, which should be done within about 10 days. The only comments on the CP received thus far are from NARA and deal primarily with retention of audit data. At it's February 12 meeting, the LPWG agreed to look into electronic record retention and address the issues raised by NARA.

Judy has also asked the LPWG to consider issues related to the FBCA cross-certifying with non-Federal entities. (The CP states, at 1.1.4, that initially the FBCA will cross-certify only with federal agencies, but that there is every intention to cross-certify with non-Federal entities in the future, at which time the CP will need to be modified accordingly.) Because several non-Federal entities (the State of Illinois, Government of Canada, and the Higher Education Bridge CA) wish to, and have CAs capable of, cross-certifying with the FBCA, the LPWG will begin investigating possible statutory or policy obstacles to such cross-certification, with the goal of revising the CP to permit the FBCA to cross-certify with non-Federal entities.

Ashley Hou (SBA) and Art Purcell (USPTO) have volunteered to co-chair the LPWG, meeting of which will be held on March 12 at the GSA NCR Bldg, room 5700, from 1:30--3:30 p.m.

The FPKIPA last met on February 6, 2001. The PA is in the process of completing its review of the form agencies will use when applying to interoperate with the bridge as well as the attendant memorandum of agreement. The PA is also revising its charter. The next FPKIPA meeting will be held on March 13, 2001 (9:00 a.m. until 10:30 a.m. at 1425 New York Ave, Room 110). Any SC member may attend PA meetings as an observer.

Brant Petrick is the webmaster for the FPKISC web site and the soon-to-be created FPKIPA web site. The new URL for the FPKISC www.cio.gov/fpkisc; the FPKIPA URL will be www.cio.gov/fpkipa and should be operational within the next few weeks.

On February 9, an FBCA status meeting was held with Mitretek, BAH and members of the FBCA TWG. A timeline for reaching a production bridge was agreed to (and has been sent to FPKISC members), with a schedule that would have the FBCA operational April 1, 2001. In discussing milestones and goals, it was acknowledged that in evaluating vendors' (Entrust and Baltimore Technologies) products we may discover some of the specifications in the CP technically cannot be met at this time, necessitating changes to the CP. Assuming no slippage in the timeline, Judy plans to present any such modifications to the CP to the Policy Authority at its March meeting.

At the FBCA status meeting, VeriSign presented a discussion of an XML-based key validation system (XKMS), which they have developed in partnership with Microsoft and other vendors. XKMS uses an assertion server to perform many tasks that the client CA would otherwise have to perform, allowing for a "thin" client. Tim Polk briefly discussed the mechanism and the SC expressed an interest in a full briefing on XKMS, which Judy will arrange.

As previously noted, the State of Illinois has expressed a desire to cross-certify its root CA with the FBCA. To that end, there was a meeting on February 6 with the State of Illinois and led by Judy on the federal side with participation by SSA, IRS, and GSA's eGovernment staff – the State-Federal Interoperability working group. The State of Illinois has a working CA (they've issued about 1,000 certificates) and has been discussing a project in which employers will file annual wage reports with SSA and IRS using Illinois-issued certificates. (Note that, unlike ACES certificates where there is a charge to the relying agency, there would be no charge to IRS or SSA for accepting Illinois certificates.) The working group is reviewing other potential common business process for discussion at its next meeting, scheduled for February 28.

The technical working group (TWG), chaired by Bill Burr, met on January 30, 2001. Discussion centered on directory issues and support for both x.500 distinguished names and domain component naming; developing cryptographic standards for symmetrical key encryption; status of a generalized HMAC FIPS and a new AES Mode of Operation standard; and key management standards. There was a presentation by Conclusive on its middleware products which it argues can serve as a bridge between applications and PKI facilities. (Full text of the meeting minutes can be found at www.csrc.nist.gov/pki/twg.) The next TWG meeting is scheduled for March 8, 2001, and will be held at Computer Sciences Corporation in Fairview Park.

The healthcare working group (HCWG) recently received DOD sign-off on the Healthcare CP. All participating agencies (DOD, VA, SSA, DHHS) have now signed-off on the CP.

The SC has received $500K from the DOD, which will be used to accomplish action plan goals. Treasury has not yet transferred the $1.5M to promote interoperability with the FBCA to GSA. Additionally, $300K for SC operations has not yet been transferred from the CIO Council budget office to SC accounts.

Judy informed the group that RSA has acquired XCert International, apparently because of their Century CA.

The 2nd annual ACES Forum was held on February 14, 2001. There was good turnout—more than anticipated—and Judy thanked all who were there.

Judy has requested feedback on the revised action plan from SC members. So far, OMB and the Environmental Protection Agency (EPA) are the only agencies that have responded.

Judy handed out a draft *Criteria for an Agency to Apply to Interoperate with the FBCA*; please provide feedback to Rebecca Kahn at rebecca.kahn@gsa.gov. Judy also asked the SC to provide comments to Brant Petrick (brant.petrick@gsa.gov) concerning his February 2 e-mail asking agencies with current PKI initiatives how many certificates they have issued and the number of certificates issued to Federal and non-Federal entities.

Judy will host the American Bar Association's (ABA) Internet Security Council (ISC) quarterly meeting April 18-19. The ISC will provide the SC with a final draft of its PKI Assessment Guide, which Judy will provide to SC members for review. Art Purcell, who has worked on the document, warned that it is several hundred pages in length and although would have been a seminal document two years ago, may not be so now. LPWG members will also review the ISC.

A Native American IT conference is scheduled for July 2001. The Indian Health Services (IHS) is participating and has asked for FPKI participation. Rebecca is scheduled to attend.

The next SC meeting is scheduled for March 14 from 1 p.m. to 3 p.m. at the GSA NCR Building, Room 5700.

Attendees:

Name	***Organization***	***E-Mail***
Peter Alterman	NIH	altermap@od.nih.gov
Ruth Anderson	VA	ruth.anderson@mail.va.gov
Lewis Baskerville	SBA	lewis.baskerville@sba.gov
Andy Boots	ED	andrew_boots@ed.gov
Russell Davis	FDIC	rdavis@fdic.gov
Tice F. DeYoung	NASA	tdeyoung@mail.arc.nasa.gov
Scott Eltringham	DOJ	scott.eltringham@usdoj.gov
Ashley Hou	SBA	ashley.hou@sba.gov
Marvin Jennings	DOD	mljenn1@missi.ncsc.mil
Rebecca Kahn	GSA	rebecca.kahn@gsa.gov
Frank Kesterman	ED	frank_kesterman@ed.gov
Mark Liegey	USDA	mark.liegey@usda.gov
Dan Maloney	VA	daniel.maloney@med.va.gov
Gene McDowell	NOAA	eugene.c.mcdowell@noaa.gov
Chuck McGann	USPS	cmcgann2@email.usps.gov
Michelle Moldenhauer	Treasury	michelle.moldenhauer@do.treas.gov
Eric Moos	DOD	eric.moos@osd.mil
Kim Nelson	EPA	nelson.kimberly@epa.gov
Manuel A. Palau	FDIC	mpalau@fdic.gov
Brant G. Petrick	GSA	brant.petrick@gsa.gov

Jennie Plante	DOJ	jeanette.plante@usdoj.gov
Tim Polk	NIST	tim.polk@nist.gov
Art Purcell	USPTO	art.purcell@uspto.gov
Judy Spencer	GSA	judith.spencer@gsa.gov
Michael White	NARA	michael.white@nara.gov
Jonathan Womer	OMB	jwomer@omb.eop.gov