Federal Public Key Infrastructure Steering Committee (FPKISC)
Meeting Minutes – April 19, 2001

Federal Bridge Certification Authority (FBCA) Status – Judith Spencer (GSA):
The plan is to be operational by mid-May 2001. Outstanding issues have been discussed and are being worked. Changes made to the x.509 Certificate Policy (CP) for the FBCA have been forwarded to the Federal PKI Policy Authority (FPKIPA) for approval. NASA and the USDA NFC will be the first two federal government agencies to cross-certify with the operational Federal Bridge (FB). Other federal government agencies that want to cross-certify with the FB must have a "live" Certification Authority (CA), and must notify Judy of their intentions via electronic mail as soon as possible.

FPKIPA Status – David Temoshok (GSA):
The FPKIPA is in the process of finalizing the following documents: x.509 CP for the FBCA, x.509 Certification Practice Statement (CPS) for the FBCA, Application for Interoperability with the FBCA, FPKI Memorandum of Agreement, and By-Laws and Operational Procedures/Practices for the FPKIPA. These documents will be voted on at the next meeting (May 15th). The Charter of the FPKIPA has been finalized, however it will be revised in the near future.

XKMS Presentation – Warrick Ford (VeriSign):
XKMS stands for extensible markup language (XML) Key Management Specification. Allows you to manage public keys with XML. XML presents the opportunity to easily add PKI services to applications. The XKMS status summary was developed by VeriSign, Microsoft, and WebMethods. It is supported by IBM, HP, iPlanet, Baltimore Technologies, Entrust Technologies, RSA, IONA, PureEdge, Evincible, CitiGroup, Reuters, SAIC, and CIBC. It was submitted to the W3C with a proposal to formally standardize. There are several vendors participating with informal interoperability testing. XKMS is compatible with x.509 (XML signature and XML encryption protocol) and has broad industry support (an open standard that doesn't verify the signature but delivers the public key). If you have any questions, contact federal@verisign.com.

Middleware Presentation – Michael Gettes (Georgetown University/Internet2):
Internet2 is a collection of 180 institutions that access a research network. If the goal is PKI, then you need to consider identifiers (SSNs), an identification process, authentication systems (Kerberos, LDAP), lawyers and policies, directories (and the applications that use them), certificate management system deployment (CA), and authorizations. Middleware is security, and the ability to build applications and system infrastructure. Higher Education (HE) is developing a CP document and will deploy a HE bridge certification authority (HEBCA) so that they can cross-certify with the FBCA.

PKI Assessment Guidelines (PAG) Document – American Bar Association Information Security Committee (ABA/ISC):
Randy Sabett gave a PAG document overview. Covers a broad range of business approaches. It is a five year project of which the group has been working on the PAG document for four and a half years. This group consists of business, legal, and technical professionals. They followed RFC2527 framework. Currently developing guidelines, and performing liability analysis. There is an internal ABA/ISC review of the public draft underway. The target date for the public exposure draft is mid-June 2001.

Business Working Group (BWG) – David Temoshok (GSA):
The next meeting will be April 24th, 9:00 a.m. at GSA HQ in conference room 5141B. This will be a special joint meeting with the Technical Working Group. There will be a lessons learned presentation by Vince McCullough (TRW).

Technical Working Group (TWG) – Bill Burr (NIST):
The next meeting will be April 24th, 9:00 a.m. at GSA HQ in conference room 5141B. This will be a special joint meeting with the BWG. There will be a presentation by Michael Gettes (Georgetown University/Internet2) on Middleware.

Legal & Policy Working Group (LPWG) – Ashley Hou (SBA):
The next meeting will be April 23rd, 1:30 p.m. at the GSA NCR Building in conference room 5700. The group will be discussing interoperability issues with the FBCA and with other PKI bridges that want to cross-certify with the FBCA.

Health Care Working Group (HCWG) – George Fortwengler (HHS):
Government agencies that have health care PKI pilot projects need to fill-out the form "Application for Funding from the FPKISC". This form was provided to the group and is also present on the FPKISC web site (www.cio.gov/fpkisc) and the FPKIPA web site (www.cio.gov/fpkipa). HRSA gave a presentation on the Federal Credentialing Program (FCP). The FCP is a federal effort to develop and deploy a single National Credentials Data Bank (NCDB) to create and store a uniform set of data elements for credentialing federal health care providers. Mitretek gave a presentation on their PKI efforts. This includes efforts involving both the federal government and the private health care sector. VHA gave a two-part presentation on the Government Computer-based Patient Record project and on the American Society for Testing and Materials (ASTM) Standard Health Care Certificate Policy. The next meeting will be April 24th, 10:00 a.m. in the HHH Building, HHS conference room 325A.

State Interoperability Working Group – Judith Spencer (GSA):
The state of Illinois is forming small groups to address applications that are needed for use by businesses once cross-certified with the FB. The state of Illinois is expecting to cross-certify with the FB early fall 2001. The following federal government agencies have participated in this working group: EPA, FDIC, FEMA, GSA, IRS, SBA, and SSA. New Jersey and Washington have expressed an interest to participate in these meetings.

Next Meeting:
The next meeting will be May 21st, 9:30 a.m. at the GSA NCR Building in conference room 5700.

Attendance List:

Name	*Organization*	*Address*
Peter Alterman	HHS	peter.alterman@nih.gov
Arthur Beller	NASA	arthur.beller@hq.nasa.gov
Bill Burr	NIST	william.burr@nist.gov
Michelle Davis	FDIC	micdavis@fdic.gov
Tice F. DeYoung	NASA	tdeyoung@mail.arc.nasa.gov
Donna F. Dodson	SSA	donna.dodson@ssa.gov
Steve Duncan	GSA	stephen.duncan@gsa.gov
Scott Eltringham	DOJ	scott.eltringham@usdoj.gov
Stan Fishkind	NASA	stanley.fishkind@hq.nasa.gov
George Fortwengler	HHS	george.fortwengler@hhs.gov
Mark Giguere	NARA	mark.giguere@nara.gov
Paul D. Grant	DOD	paul.grant@osd.mil
Ashley Hou	SBA	ashley.hou@sba.gov
Marvin L. Jennings	DOD	mljenn1@missi.ncsc.mil
Rebecca Kahn	GSA	rebecca.kahn@gsa.gov
Frank Kesterman	ED	frank_kesterman@ed.gov
Dinesh Kumar	SSA	dinesh.kumar@ssa.gov
Mark Liegey	USDA	mark.liegey@usda.gov
Gene McDowell	NOAA	eugene.c.mcdowell@noaa.gov
Chuck McGann	USPS	cmcgann2@email.usps.gov
Jan S. McNutt	DISA	mcnuttly@ncr.disa.mil
Russell C. Moritz	DOL	moritz.russell@dol.gov
Dara Murray	NSF	drmurray@nsf.gov
Brant G. Petrick	GSA	brant.petrick@gsa.gov
Jennie Plante	DOJ	jeanette.plante@usdoj.gov
Shauna Russell	DOD GC	russells@osdgc.osd.mil
Judy Spencer	GSA	judith.spencer@gsa.gov
David Temoshok	GSA	david.temoshok@gsa.gov
Mark Watson	FDIC	mawatson@fdic.gov
Kent Weitkamp	SSA	kent.weitkamp@ssa.gov
Michael White	NARA	michael.white@nara.gov
Jonathan P. Womer	OMB	jwomer@omb.eop.gov
Lee Zeichner	CIAO	lee.zeichner@ciao.gov