Federal Public Key Infrastructure Steering Committee
Minutes of the December 1, 2000 Meeting
GSA Building, 7th & D Streets, SW, room 5700

The meeting convened at 9:37 a.m. Thanks to Kim Nelson, Judy Spencer and Denise Silverberg for the holiday goodies. Thanks to Judy and Trudy for the coffee, tea, and apple cider mix.

This was Rich Guida's last meeting as Chair; Judy Spencer, GSA, will be taking this position starting in CY2001. Rich thanked the Steering Committee for the pleasure and honor of working with them – a group of high quality people working with determination on complicated issues. He expressed his view that as a consequence of the work of the members, within the Steering Committee and individually within their agencies, there has been substantial progress in the use of public key technology government-wide. He expressed his heartfelt thanks to the members.

Rich Guida provided the status of several ongoing activities:

Status of Funding Request in FY01 Budget: The continuing resolution continues as of this date. Until Congress reconvenes, we won't know how the Treasury bill will fare. We expect the $3.5M request to be approved for the FBCA, FPKI PA and agency cross-certification with the Bridge. It had been hoped that these funds would have been available and dispersed by now. If and when the funds are approved, our staff – who will transition to work with Judy Spencer – will work with OMB as discussed at the October meeting.

Status on the Federal Bridge: The Entrust node is operational and stable. Baltimore's latest production software did not support PKCS 10 v1.7; the alpha version does but is not stable. Baltimore has promised a stable beta version in December. This compounds the delay in getting the prototype re-operational to the end of the year. We expect the production version to be operational early next year. The plan is for the production FBCA to contain other CA products, which would be tested within the prototype prior to incorporation. Hopefully this will happen once Congress approves the funding.

Number of Efforts Underway:

The framework for the Policy Authority is in place (FPKI PA). The Certificate Policy (CP) goes before the PA at their December 19th meeting. Lee Holcomb, Co-Chair, Enterprise Interoperability and Emerging Information Technology Committee (EIEITC), wants to get the CP to the Federal CIO Council soon thereafter.

The FPKI PA By-Laws and draft Memorandum of Agreement (MOA) and application form are or have been circulated for review by the PA. The Guide to Interoperability with the FBCA is going through PA review now. The plan is for the Policy Authority to have its own website; for now, the PA activities are on the Steering Committee website. NIST has offered to post the PA documents on a website there, temporarily.

Judy Spencer will be developing where the Steering Committee needs to go in 2001. The sooner Agencies apply to interoperate with the Bridge and begin that work, the sooner we will tease out the issues involved in doing so. The only way to make this successful is to test whether the process is too onerous; think through or walk through the various steps and provide constructive comments back to the Steering Committee.

Rich's next Career: Rich announced that he will be going to work for Johnson & Johnson in their medical devices and diagnostics area as a corporate IT security director, deploying comprehensive PKI throughout the 180 companies comprising J&J. J&J has its headquarters in Brunswick, NJ.

Meeting with U.K. PKI Counterparts, London, England: The U.S., Canadian, and Australian PKI representatives met with our UK counterparts for the week of October 30th – November 3rd. On the first day we met with folks from ETSI, EESSI. They are putting together rules for the European Community for PKI. The European Community has very strict rules on what is a qualified signature and for accepting them. These standards apply to doing business within the EC. As individual nations, each nation can do as it will. There are disconnects between us. As a first step in working these, we have agreed to review each other's documents, identify common ground, properly define our differences, and then meet again to work on those differences.

The European Community is looking at every type of transaction (b2b, b2c, g2c, etc.). And the EC nations are setting up licensing offices in each nation to assure that their CAs are issuing qualified certificates. It is a more prescriptive model than the USA's.

The rest of the week, each nation gave briefings on their initiatives. There was a good exchange of information and a lot of commonality. The Australian Tax Office's CA (equivalent to our IRS) is online and issuing certificates. The U.S. Government use of PKI is equivalent to or more advanced than the other countries we've met.

The UK is setting up their system around life events for dealing with the public, and through a portal – come into a central point and register for services desired, then authenticate to or at the portal. (The UK government is thinking of getting rid of all agency websites.) The US approach is a communities of interest approach from the provider perspective. The Canadians conduct their ID proofing at the application layer.

On Thursday, November 30th, Judy Spencer and Denise Silverberg met with a representative from the New Zealand government. Their government is smaller than USPTO. New Zealand is looking to institute an enterprise-wide PKI, initially for g2g business internally. NZ is also debating whether to obtain certificates from the Australians or do something themselves.

Rich summed up this discussion with: These meetings are setting the stage for intergovernmental interoperability. How will the countries interoperate on a policy and technical level? Yet to work out the details. These early conversations are worthwhile for somewhat influencing each other approaches to facilitate that interoperability. Within each government,

there is a body equivalent to the FPKI PA. Likely that the FPKI PA would invite representatives of the other bodies to meet with them.

ACES: The NIST Task Order was awarded – a grants, advanced technology program – to AT&T for a complete PKI implementation for a grants application website. NIST expects to launch that website in a year. Also a second RFP for NIH is on the street. This is a follow-on to their first RFP. NIH has two pilot applications, one internal and one external.

Debate with the Academic Community re: anonymous or pseudonymous certificates. With the public, this approach is understandable. The academic community asks why not use these for every transaction. Relative to business and government transactions, especially relative to court cases, these types of certificates would complicate prosecution. Rich's discussion with the Higher Education PKI group (November 29th in Washington, DC), in part, focussed on how much additional complexity was injected by anonymity. The Dept of Justice GPEA guidance was signed out by Attorney General Reno last Wednesday.

Technical Working Group, 11/2/00: Kathy Lyons-Burke reported for the Chair, Bill Burr. She passed out the minutes. The meeting focussed on roaming solutions. See the TWG web page for copies of these minutes. The next meeting is scheduled for January 10, 2001.

Business Working Group: Five agencies gave presentations on best practices. There were 27 attendees from a broad range of agencies. The next meeting is scheduled for January 8, 2001 at 9:30 a.m. at GSA HQ, room 3240. SSA and VA will present a risk assessment document published by SSA, and DOD will present a best practice. As an outgrowth of the past meeting, USPTO is investigating the FDIC best practice as a remedy for their work-at-home program; evidence of the immediate value of these exchanges.

The meeting formally adjourned at 10:45 a.m. Members remained for a time longer to visit, say goodbye, and eat up the nut cookies, chocolate fudge (Kim is famous within the SC for this), brownies and Pepperidge Farm cookies available.

Judy Spencer will announce the date of the next FPKISC meeting.

Attendees who signed in:

Richard Guida	Treasury and outgoing Chair, FPKISC
Denise Silverberg	Treasury and Deputy to the Chair
George Thurmond	Georgia Technology Agency, Georgia Tech
Peter Alterman	NIH/DHHS
Nelson Barry	DOE
Roger Bezdek	Treasury
Russ Davis	FDIC
Tice DeYoung	NASA-ARC
Scott Eltringham	DOJ
Mark Giguere	NARA
Paul Grabow	FRB

Louis Grosman	NRC
Mark Liegey	USDA
Kathy Lyons-Burke	NIST
Gene McDowell	NOAA
Mary Mitchell	GSA
Michelle Moldenhauer	Treasury and Chair, FPKI PA
Kimberly Nelson	EPA
Michael O'Leary	DOJ
Arthur Purcell	USPTO
Kathy Sharp	USDA(NFC)
Judith Spencer	GSA and incoming Chair, FPKISC
Shahira Tadross	DOJ/EOUSA
Barry West	GSA
Francine Yoder	DOJ
David Temoshok	GSA
Jeanette Plante	DOJ
Richard Nunno	CRS
Clarissa Reberkenny	DOD