Federal PKI Steering Committee Meeting
May 7, 2003

There were five responses to the 2003 Application for FPKISC Funding. Four of which were approved for funding since they were cross cutting organizations: USDA/NFC (payroll systems), DOD (Microsoft Outlook email client), GSA (multi-use client for email and path discovery) and HHS/NIH (form signing across different applications for the NIH/Educause project).

Judy gave a presentation on “Federal PKI: The Next Generation”. A lot has been going on the past couple of months with Federal PKI and a lot of work is being done with the CIO Council. OMB proposed an Authentication and Identity Policy Framework for Federal Agencies, which will be a subset of the e-Authentication initiative. If your agency is a partner in the e-Authentication initiative, your agency’s CIO senior executive will be getting information this Friday (May 9th) about establishing an e-Authentication Executive Steering Committee which will be attended by Mark Forman. Membership of the e-Authentication Executive Steering Committee is reserved to the initiatives funding partners.

The E-Gov agenda has twenty-four initiatives. The Common Policy framework should take care of Internal Efficiencies and Effectiveness (IE&E). IE&E pertains to the government’s internal functions (e.g. financial management, payroll, travel) as well as externally (with other federal agencies).

Identity management principles for Federal agencies will consolidate on a credentialing process for physical and logical credentials for building access, system access, and digital signatures. The Federal government will soon be requiring the use of a common certificate policy for Federal PKI systems. OMB will be establishing a policy to establish a consistent way to authenticate and identify Federal employees. The development of the common policy framework will be overseen by the newly formed e-Authentication Executive Steering Committee. The Federal CIO Council Architecture and Infrastructure Committee will endorse the standard authentication component.

The basic assumption for a common PKI policy applies to Federal employees, contractors, and affiliates. Federal organizations that are cross-certified with the FBCA at the medium level of assurance are compliant with the common certificate policy. Unified physical and logical access implies hardware token deployment (smart cards). However, hardware tokens are not stipulated.

Issues associated with “The Next Generation” common policy framework for Federal identity management will be largely PKI based. However, its scope encompasses more than just PKI, an interagency body must be constituted to make this common policy framework a reality. A solution would be to: leverage the current infrastructure available in the FPKISC, expand its scope to encompass the needs of the common policy framework, and add capabilities from other stakeholder groups.

It looks as if the FPKISC will be renamed the “Federal Identity Management Committee”. This will realign the FPKISC to reflect current activities government-wide. There will be a continuing role for the Federal PKI Policy Authority and the FBCA Operational Authority. We’ll be expanding the focus to include related activities and groups. These include: smart cards, building security, and human resources. Also, we’ll provide policy guidance for the development of other identity management technologies in addition to PKI and smart cards, continue activities of the Federal PKI Technical Working Group, and stand up ad hoc focus groups to tackle specific issues.

The OMB e-Authentication guidance defines four levels of assurance. Levels three and four require cryptographic solutions. NIST technical guidance will accompany OMB guidance.

A common policy for physical and logical credentialing of Federal employees is needed. This requires a credential (smart card) policy. A set of minimum requirements for identity assurance for Federal employees is also needed. At a minimum, it requires Human Resources identity guidance. A common policy for PKI deployment to Federal employees would be based on the FBCA CP at the medium assurance level. Last but not least, a consolidated acquisition for implementation is needed. We would need to identify a set of approved providers under the guidelines above, and gather organizational requirements.

The role of the FBCA will continue to: bridge between the Federal PKI and external organizations, bridge between enterprise PKIs within government, and enable external PKI interoperability with the Federal e-Authentication gateway (a relying party).

Judy also discussed milestones as they pertain to identity policy, aggregated buy, and shared service migration. In summary: the FPKISC will be transformed into the Federal Identity Management Committee, new players will be invited to the table, a letter will be sent to the Federal CIOs explaining the change as well as requesting official designation of representatives to support the new committee, current initiatives involving the FBCA will continue, and we’ll be on the fast track to have results by November 2003.

A revised draft of the CP for the Common Policy framework will be emailed to the FPKISC members for their comments. All previous comments from federal agencies have been incorporated into this release. Ninety percent has already been approved in the FBCA CP, while ten percent of it is new. Please pay close attention to the identity proofing sections in the new release. By year 2009, Federal agencies will be required to use 2048 bit cryptographic keys and the SHA-256 hashing algorithm.

An email message will be sent to FPKISC members with details for the next FPKISC meeting. As always, government contractors are not permitted to attend FPKISC meetings.

Attendees:
Judith Spencer, FPKISC
Brant G. Petrick, FPKISC
Peter Alterman, HHS/NIH
Gene McDowell, NOAA
Jeanette Thornton, OMB
Art Purcell, USPTO
Tin Cao, DOS
Michael Ball, DOJ
Nancy DeFrancesco, DOC
Tice DeYoung, NASA
Jan S. McNutt, DOD
George Fortwengler, HHS
Bill Burr, NIST
Tim Polk, NIST
Lewis Baskerville, SBA
Donna Dodson, SSA
Bob Donelson, DOI
Paul D. Grant, DOD
Debbie Poff, FAA
Bill Holcombe, GSA
Lolie Kull, DOS
Amy Bunk, NARA
Kevin Green, NARA
Peter Batista, DHS
Carlos Santana, DOL
Meng Lin, DOJ
Jim Osterritter, DOD
LaKeishia Dubose, DOL
Von Harrison, GSA
Kathy Sharp, USDA/NFC