

Steering Committee Minutes

May 22, 2000

Location: GSA NCR Building, 7th & D Streets, SW

Introduction

Rich Guida, Chair of the FPKISC, convened the meeting at 9:35 AM.

General Updates

Rich reported on the following efforts:

Conversion to CIO Council:

Rich advised that the Steering Committee is now officially under the Enterprise Interoperability and Emerging IT Committee of the CIO Council, with strong ties to the Security, Privacy and Critical Infrastructure Committee. This represents the expected transition and is extremely good news that it has been consummated.

FPKI Policy Authority:

The initial six charter members of the FPKI Policy Authority include the Office of Management and Budget, Department of the Treasury, General Services Administration, Department of Commerce, Department of Justice and the Department of Defense. A letter will be distributed to all Agency/Department CIOs establishing the Policy Authority and identifying the initial charter members, citing the draft charter which was previously adopted by the Steering Committee. The Policy Authority must establish the policy mappings between the FBCA and applicant agencies. The voting members of the Policy Authority will expand to include all Agencies/Departments who are approved to interoperate with the FBCA. All members of the FPKISC may participate in the Policy Authority as non-voting members until they are accepted as voting members.

PKI Status Report (“The Evolving Federal PKI”):

The final version of the PKI status report was distributed electronically last night, containing previously received input from every Agency/Department that provided input. It is now ready for final review and updates. Agencies were requested to provide any final input by the end of May so the document can be finalized and send to the publisher.

Federal Bridge Certification Authority (FBCA):

As previously reported, the prototype of the FBCA went operational in February. As a result of the successful effort of the EMA Challenge, Rich and others met with senior DOD officials to seek their support to accelerate development of the production version of the FBCA. DOD agreed to provide \$500K in FY01, and based on that, GSA plans to spend that amount this fiscal year out of their working capital funds (reimbursed next fiscal year) in order to get a two-node production FBCA operational hopefully by later this summer. Rich expressed deep appreciation to DOD, and to Lee Holcomb and John Gilligan of NASA and DOE respectively, for their efforts in supporting this work.

In addition to this, Baltimore will be replacing the Cybertrust node of the prototype FBCA with their Unicert product. Mitretek is developing a plan of action for this as well

as for developing the production FBCA, and for supporting testing with the NSA Bridge Demonstration Phase II work. The production FBCA will be constructed at a GSA facility, most likely the NCR building at 7th and D Street SW.

FBCA Certificate Policy (CP):

The Certificate Policy (version 1.4R) was distributed for comment on 4 March 2000. A large number of comments were received requesting additional modifications and/or changes. Joe Mettle composed a Comment Resolution Document (78 pages) that defines each comment received, who was the author, date, time, subject and resolution. This document will be distributed to the FPKISC members within the next two weeks. Rich and Joe expressed deep appreciation for all of the comments received. Joe Mettle also updated the Certificate Policy to reflect the comments received. The next version of the Certificate Policy will also be distributed within the next two weeks, with a goal of finalizing the document by July. (Subsequent to the meeting, an updated version was circulated but owing to the large number of comments, many of which were divergent, additional effort will be needed to reconcile the differences.) Rich emphasized that the FBCA Certificate Policy will need to be made coherent with the DoD Certificate Policy so that there is a clear mapping which both DOD and the FPKIPA find acceptable.

Personnel:

Johnny Sumners will be departing at the end of the month. A replacement is being interviewed. Further, two of the detailees on Rich's staff are scheduled to depart within the next six weeks, and a third later in the summer, so resources are limited.

Budget:

As previously reported, Treasury has \$7M in the FY-2001 budget to support the production FBCA, the FPKI Policy Authority, and Agencies/Departments that are currently piloting PKI initiatives. Rich reported that the budget request is going through the Congressional review process, thus far with mixed results. Rich promised to report progress as it occurs.

Rich then asked Judith Spencer to brief the Steering Committee on the Status of ACES.

ACES:

GSA awarded two contracts acquiring 500,000 certificates with no initial issuance fee. Digital Signature Trust was awarded a contract to provide 400,000 certificates that would be valid for six years. AT&T was awarded a contract to provide 100,000 certificates that would be valid for two years. Participating Agencies/Departments will pay for certificate use per the standard ACES model. The certificates will be ready to be distributed beginning in the June time frame. Agencies/Departments interested in acquiring any of the certificates should contact Judith Spencer at GSA. Rich requested the Chairpersons of each Working Group to report on their efforts.

Test Working Group (FPKISC-TWG)

Bill Burr distributed the minutes of the TWG meeting conducted on 11 May at NOAA. Major items discussed include:

- (1) A digital Signature/workflow application
- (2) EMA Challenge Report
- (3) Certificate and CRL Profile
- (4) Directory Interoperability Profile
- (5) Advanced Encryption Standard status

Legal Policy Working Group (FPKISC-LPWG)

Michelle Borzillo reported that the LPWG has developed a draft application form for agencies to use in applying for interoperation with the FBCA - that is, to map an agency's CP to the FBCA CP. Michelle requested comments from Steering Committee members, and especially from the TWG as to the technical content of the form.

Business Working Group (FPKISC-BWG)

Barry West recently joined the Business Working Group working for Mary Mitchell, who is co-chair of the BWG; Barry will be assisting Mary to re-invigorate the group in the near future.

Open Discussion

Policy Authority Responsibilities:

While the FPKI Policy Authority will perform policy mapping, there has been considerable discussion over what, if anything, the Policy Authority should require of applicant agencies concerning their directories. The unanimous consensus was that the Policy Authority should provide assistance to applicant agencies in understanding what they should do to interoperate with the FBCA directory (and thus be able to have their client software make use of the certificates issued by the FBCA as was demonstrated by the EMA Challenge), but that the Policy Authority should not require directory interoperability as a precondition to getting an FBCA certificate. The TWG will review this area and develop what information would be helpful to agencies attempting to effect directory interoperability for this purpose.

Conclusion

The meeting was adjourned at 11:50 P.M. The next meeting will be on 10 July, from 1:00PM to 3:30PM, at GSA (same location).