Steering Committee Minutes
February 28, 2000

Introduction

Rich Guida convened the meeting at 9:35 AM. Upon completion of general introductions of the attending members, Rich introduced Mr. Steven Akridge from the State of Georgia. During a recent business trip to Georgia Tech Research Institute, Rich invited the State of Georgia to attend FPKISC meetings as an ex officio member because they are interested in exploring the uses of PKI and had expressed an interest in keeping track of activities underway in the Federal Government. This is consistent with invitations extended to other state governments as well.

General Updates

Rich reported on the following efforts:

Disestablishment of the GITS Board

The Office of Management and Budget and the National Partnership for Reinventing Government established the Government Information Technology Services (GITS) Board to spearhead the Access America initiative. For a variety of reasons, the GITS Board is being disestablished, and its activities will be folded into the Federal CIO Council, which has a statutory (Clinger-Cohen) charter. The Steering Committee will be transferred to one or both of the Security, Privacy, and Critical Infrastructure Committee, and the Enterprise Interoperability and Emerging IT Committee. The Federal PKI Policy Authority will also will be established under one or both of those committees. The transition is expected to be completed by this summer.

Federal Bridge Certification Authority (FBCA)

Rich complemented Judith Spencer of the General Services Administration and Mitretek for their outstanding efforts developing the FBCA. The prototype FBCA went operational February 8, 2000, and the plan is to have a production version (with additional CA products inside the membrane) operational by late 2000. Rich noted that CIO Council members had expressed a desire to provide resources to accelerate development of the production FBCA, and that possibility is currently being reviewed. Rich then suggested that if Agencies desire to cross-certify with the prototype Bridge in order to test their PKIs and applications, we would be prepared to work on that. Any interested Agencies must contact Judith Spencer no sooner than the middle of April (i.e., after the EMA Challenge is over - see below) to make arrangements. Cathie Ward, Verterans Affairs, expressed an interest to cross-certify a Verisign CA with the FBCA in order to test some Veterans Administration functions.

Electronic Messaging Association (EMA) Challenge 2000

The FBCA and DoD Bridge will test interoperability across the most complicated PKI ever attempted in either industry or Government, specifically covering six PKI domains (with one domain, that of DOD, itself including three disparate sub-domains). The objective of the Challenge is to demonstrate the capability for the recipient of an signed S/MIME e-mail message to develop a certificate trust path from the PKI domain of the recipient to the PKI domain of the sender, and then validate the signature on the message by processing all of the certificates in the trust path to ensure none has been revoked. The components and architecture are as follows:

FBCA Bridge
Entrust Certification Authority (CA) cross-certified with CyberTrust CA
CyberTrust CA cross-certified with Entrust CA
X.500 Chained Directory

DOD Bridge
Cygnacom CA as the DOD single-CA hub
Entrust CA mesh cross-certified with Cygnacom CA
Spyrus CA hierarchy cross-certified with Cygnacom CA
Motorola hierarchy cross-certified with Cygnacom CA
CyberTrust cross-certified with Cygnacom CA
X.500 Chained Directories

National Institute of Standards and Technology (NIST)
Entrust CA cross-certified with the Entrust CA within the FBCA membrane
Entrust CA cross-certified with the CyberTrust CA in the FBCA membrane
Eudora S/MIME mail-client configured to interoperate with Entrust CA
Eudora S/MIME mail-client configured to interoperate with CyberTrust CA
X.500 Chained Directory

Government of Canada (GOC)
Entrust CA cross-certified with the Entrust CA within the FBCA membrane
Eudora S/MIME mail-client configured to interoperate with Entrust CA
X.500 Chained Directory

General Services Administration (GSA)
CyberTrust CA operated by CitiBank to support GSA FTS
CyberTrust CA cross-certified with the CyberTrust CA in the FBCA membrane
Eudora S/MIME mail-client configured to interoperate with CyberTrust CA
X.500 Chained Directory

In addition to those agencies identified above, the Georgia Tech Research Institute and NASA are also preparing to participate in the EMA Challenge. It is anticipated, time permitting, we will be able to include them.

Future Demonstrations
The EMA Challenge 200 will only address digital signatures; future demonstrations will include encryption and policy mapping. Potential future demonstrations may include the following:

EMA European Challenge, London, June 2000
EMA Asian Challenge, South-East Asia, Fall 2000

NIST/NSA Computer Security Conference, October 2000
RSA Conference, April 2001

Funding Issues

Rich reported that the Treasury budget includes a line item of $7M for FY-2001. If the line item is approved, $2M will be used for the FBCA development and operation of the FPKI Policy Authority. $5M will be used to support Agency PKI efforts. The FPKISC with final agreement from OMB will select which agency projects to support. Rich noted that once it becomes clearer whether the funding request is surviving the appropriations and authorization processes, agencies will be asked to submit proposals in sufficient time to allow careful consideration, and to support the development of interagency agreements so that funding can be transferred to the recipient agencies quickly after the new fiscal year begins. Rich emphasized that this funding will be for projects that agencies are investing their own money in - in other words, to expand and accelerate agency efforts rather than to start them.

Digital Signature Guidance

The Digital Signature Guidance document, which tiers off of the OMB guidance being issued under the Government Paperwork Elimination Act, was circulated in December 1999 and is currently undergoing review. Rich encouraged agencies to supply any final comments as soon as possible so the document can be finalized and issued at the same time as the final OMB electronic signature guidance, which is scheduled for April 23, 2000.

FBCA Certificate Policy (CP)

The CP was distributed for comment on December 30. To date we have received about 270 comments. Joe Mettle composed a document that defines each comment received, who was the author, date, time, subject and resolution. This document will be distributed to the FPKISC members next weekend. Joe also updated the CP to reflect the comments received and resolution. The next version of the CP will also be distributed next weekend. We are requesting the FPKISC members to review the revised CP and provide us comments by the next Steering Committee meeting.

PKI Forum

The PKI Forum is an industry generated entity, web site www.pkiforum.org. Their first public meeting was held during the recent RSA conference. The mission of the Forum is to test interoperability among different PKI CA products, directories and clients. The Forum is an open organization; individuals, organizations, and companies may join. There are several levels of membership and joining fees, each of which has different privileges. Rich stated that in conjunction with the Government of Canada, we are asking the Forum to create a separate "government" membership level for Government entities. This new level would not have a membership fee and the Government representatives would not be voting members. The Forum has this matter under consideration and it will be discussed further at a March 6th meeting in San Francisco which Rich is attending.

KRDP
The KRDP Interagency Agreement is almost in place with SSA. We are still working with Dept. of State to complete the IA with them.

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

Judith Spencer (GSA)
The ACES Customer Advisory Board is meeting on Tuesdays to ensure ACES is moving in the right direction. The next meeting will be on March 8, 10 A.M., at the Hubert Humphrey Building.

GSA has approved the Social Security Administration as the first Designated Procurement Authority, which allows them to administer ACES task orders directly rather than through GSA.

One of the ACES vendors has proposed an unfunded task order to produce 500,000 certificates and place them in a bank. The fees would be paid when the certificates are issued.

Access America for Students is expected to issue two task orders, the first one in April.

The certification of one or more of the ACES vendors may be completed by the end of March, thus allowing ACES certificate issuance to commence.

The Certificate Arbitrator Module (CAM) is operational. The CAM code may become Open Source by the end of March. The Government of Canada, City of Los Angeles/County and Industry Partners have expressed an interest in building similar CAMs.

Open Discussions

Peter Weiss (OMB)
Peter is moving on to NOAA Weather Service to work international policy issues.

Jonathan Womer will be taking over for Peter.

The GPEA final guidance is expected to be released in April as required by GPEA.

OMB noted that during the FY01 budget rollup, several agencies had requested money for PKI projects, but when OMB asked some simple questions, the requests evaporated. OMB ascribed this to agency budget offices making decisions to cut the requests without understanding the need for the projects. OMB strongly encouraged agency program personnel who fashion such requests to explain PKI to their budget colleagues, and to defend against efforts to cut the funding. OMB noted that had the agencies stuck by their initial requests, it is likely that they would have received some or all of the PKI funding they sought.

Cathie Ward
The FedCIRC CERT currently uses PGP for encrypted e-mail for convenience since an interoperable PKI which would support S/MIME transactions is not yet available.

VA believes that the use of PKI is preferable to PGP, and that position was strongly supported by others present since PKI provides greater discipline and structure for certificate management.

A suggestion was raised for the Veterans Administration to draft a letter which the Steering Committee would send to the CERT encouraging the use of PKI rather than PGP.

Other Updates

Commerce Dept
The Department of Commerce Electronic Signature/PKI Affinity Group under the CIO is investigating setting up an ACES CAM for their agency that could be relied upon by the Commerce Bureaus. A survey was taken to identify the use of electronic signature and PKI by the Bureaus and a Commerce Certificate Policy is being worked on.

The Patent Office (PTO) currently supports a PKI that services their trading partners (e.g.,i.e., patent attorneys, inventors, etc.). They have issued over 163 certificates. The certificates were used more than 23,000 times over a two-month period. The certificates support authenticated confidential patent application status inquiry and confidentiality and signature for electronic filing of patent applications.

The PTO will expand the filing pilot to include other PTO transactions in August 2000 with full production being planned for February 2001. This represents an acceleration of the original planed date due to changes in the patent laws that make electronic submission an economic and practical necessity.

PTO expects to issue between 6,000 and 10,000 certificates before the end of 2000.

NASA
NASA has completed the early stages of implementing their agency-wide PKI. They plan to issue 13,000 certificates.

FDIC
The FDIC is considering replacing their laptops with ones that are smart card enabled to support their PKI solution.

They are planning on installing certificates on their identity badges.

U.S. Navy
The U.S. Navy expects to field their pilot PKI this year.

They eventually plan to issue 800,000 smart cards.

The Navy offered to give a presentation of their smart card pilot program during the March FPKISC meeting.

Business Working Group
Richard Guida introduced Mary Mitchell of the General Services Administration as the new co-chair of the Business Working Group. Mary will be working to re-establish the BWG shortly with a new, revised charter and focus.

Miscellaneous
NARA guidelines on electronic record keeping will be released during April.

Actions
Distribute EMA Project Plan to PKISC members

Publish a report on MitreTek's activities after the EMA Challenge

Publish a monthly status report (bullets) on the FBCA, include it in the minutes

Conclusion
The meeting was adjourned at 12:00 P.M. The next meeting will be on March 20, 0930 - 1200, at GSA (same location).