Steering Committee Minutes
July 10, 2000
GSA NCR Building, 7th & D Streets, SW

Introduction
Rich Guida, Chair of the FPKISC, convened the meeting at 1:00 P.M.

General Updates
Rich Guida:

FBCA Policy Authority (FPKIPA):
The initial six charter members of the Federal PKI Policy Authority are the Office of Management and Budget, Department of the Treasury, General Services Administration, Department of Commerce, Department of Justice and the Department of Defense. The Charter and a draft distribution memo has been provided to the chair of the Enterprise Interoperability and Emerging IT Committee; once signed, it will be sent to the charter agencies, requesting each to identify its respective representative so that the FPKIPA can commence operation. It is hoped that will happen shortly.

"The Evolving Federal PKI" Report:
The content of the report was frozen as of June, and we have been going through formatting modifications since then preparatory to publication, which we hope will result in hard copies by August. A copy of the pdf version of the document, in final format, has been placed on our web site.

FBCA Certificate Policy (CP):
A subset of the Steering Committee members met at the Department of Energy in Germantown on 26 June to review the current version of the FBCA CP. We completed reviewing about half of the CP, paragraph by paragraph. We expect to meet again on 4 August to review the second half of the CP. At the completion of the next review, a polished version of the CP will be distributed to the full membership of the Steering Committee for final review.

Use of RSA with PKCS#1 in FIPS 186:
Rich drafted a letter to Bill Burr at NIST requesting an extension to the waiver authorizing the use of RSA with PKCS#1 beyond the 18 months currently provided in FIPS 186. All Steering Committee members were asked to provide any comments on the draft as soon as possible.

SSA:
Rich had a meeting at the Social Security Administration (SSA) earlier this morning, to discuss their plans for the use of PKI in a variety of applications. The meeting was very constructive and offered a further opportunity to ensure SSA was made aware of the status of ACES.

GPEA Digital Signature Guidance:

We received numerous comments from the Office of Management and Budget and the Department of Justice on the latest version of the GPEA digital signature guidance; all of those comments are under review and will be incorporated or resolved prior to finalizing the guidance. Once the guidance is finalized, it will be provided to OMB for transmission to NIST, where it will be issued as a "special publication."

Web Page:
The Steering Committee web page is undergoing a complete remodeling reflecting our transition to the CIO Council, and the need to make the page content more easily useful. We hope to have an updated version available shortly.

Judith Spencer (GSA):
President Signs E-Sign Bill S.761: President Clinton signed the E-Sign Bill S.761 using a digital signature (private key on a smartcard) with a certificate provided by Digital Signature Trust, Inc. The Bill becomes effective 1 October 2000. The certificate was acquired via the ACES contract vehicle, thus being the first production ACES certificate. The certificate was revoked after the signing ceremony. Thus, this represents a watershed for PKI in general and ACES in particular. The graphics involved during the signing ceremony will be placed on a CD for distribution to interested individuals.

Art Purcell distributed a copy of the Congressional Record providing the legislative history on S.761. Art will also provide a copy of the pertinent URL for the Congressional Record. We strongly suggest everyone read S.761 very carefully; we will discuss it in greater detail during the next FPKISC meeting.

Two requests to the ACES Customer Advisory Board (CAB) for "free-issuance" certificates were approved, one for 100,000 (Department of Veterans Affairs) and the other for 10,000 (Federal Emergency Management Agency). The ACES website (www.gsa.gov/aces) explains how to apply for ACES CAB "free-issuance" certificates.

Elaine Rimel (USPS):
The US Postal Service's first PKI application is "PC Postage". This involves generating two dimensional barcodes that are applied to mail in place of stamps. Certificates are issued to commercial vendors who produce postal devices for generating barcodes. The certificates are not published in directories. PC Postage went live last August. USPS has generated 100s of thousands of certificates which are used in the postal security devices. The certificates are used for signing each indicia generated. The USPS has sold one million postmarks with an option to sell one million more to a commercial vendor. EPMs are also generated in USPS applications such as PostECS.

Kathy Sharp (USDA):
The National Finance Center (NFC) has been using an Entrust based PKI since 1997. They are currently expanding their PKI capabilities. They are considering using the Entrust TruePass product for providing roaming capabilities. Entrust will be invited at a future Steering Committee meeting to present the functions and features of TruePass in order for all of the members to gain a better understanding of the product. This is

particularly relevant since several civil agencies are using Entrust. However, other vendors will also be invited to present information on their roaming solutions in future meetings of the Steering Committee and/or the Technical Working Group, to ensure equitable coverage.

The NFC is planning on changing the Thrift Savings Program (TSP) contribution/distribution on a daily basis. Certificates will be used to identify customers.

CIO Council:
The CIO Council has identified three Plan Objectives that involve PKI:

Objective 1.3 – Issuing certificates in the hands of users (100,000 by 01/01/01)

Objective 1.5 – Cross-Certify five different vendor CA products

Objective 3.1 – Develop a Government wide PKI during CY 2002

The second and third objectives are being revised to more accurately reflect Steering Committee efforts; a final version will be provided at a later date.

Guest Product Vendor - Litronic
Litronic has approximately 130 employees and has been in business for 25 years servicing the needs of the Government, the Financial and the Healthcare industries. Litronic emphasized that PKI can be used to protect corporate information assets. The U.S. Department of Defense uses Litronic drivers to support the largest single E-mail system in the world. It is easy to install and is complementary to existing systems. Litronic smart cards use 32 bit RISC processors and perform all cryptographic processes on board. Litronic smart cards work with a variety of CA products, card readers, etc. Litronic customers have expressed an interest in the following features of PKI systems they plan on installing:
- Easy to install
- Easy to use
- Easy to manage
- Complimentary to the way people do business
- No proprietary processes
- Support commercial open standards
- Provide total security
- Easy determination whether or not a document or e-mail was digitally signed

Technical Working Group (TWG)
NIST distributed a document for review. Everyone is encouraged to read the document and provide their comments. The document will be discussed at the next TWG meeting on 10 August at the USPTO.

Conclusion:
The meeting was adjourned at 03:00 P.M. The next meeting will be on 2 August, from 1:00pm to 3:30pm, at GSA (same location).