Steering Committee Minutes
August 2, 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 provided the following updates:

FBCA Policy Authority (FPKIPA):
The Charter has been accepted and the draft distribution memo has been signed-off on 24 June by the chair of the Enterprise Interoperability and Emerging IT Committee of the CIO Council. Two of the six charter member agencies have already named their respective representatives: Jonathan Womer (Office of Management and Budget), and Michael Duffy (Department of Justice). The first FPKIPA meeting will be held on 31 August, from 8am until 9:30am, at 1425 New York Ave, Room C110.

"The Evolving Federal PKI" Report:
The final blue-copy is correct, visually acceptable, and has been signed-off. It will be handed-off to the printers this afternoon. A copy of the pdf version of the document, in final format, has been placed on our website. Hard-copies will be ready later in August.

ARCOT Systems Roaming Solutions Briefing:
Several members of the Steering Committee participated in a meeting with ARCOT Systems on 1 August, from 9am to 11am, at NIST. We now have a clearer understanding concerning how their software protects the private key in a roaming scenario, and how their approach interoperates with different CA vendor products. Basically, the ARCOT approach for a closed PKI (where the universe of users holds certificates that are ARCOT –enabled, meaning the standard X.509 certificate is wrapped into an ARCOT credential) provides additional protection because it controls access to user's public keys (the user public keys are not publicly available); however, when a closed PKI interoperates with an open PKI (i.e., where the certificates are publicly available), that security advantage is lost. Nonetheless, the ARCOT-enabled certificates are interoperable – i.e., the holder of an ARCOT credential can interoperate with a traditional PKI since the X.509 certificate is intact. This means that users who want to send e-mail to the ARCOT credential-holder can obtain the X.509 certificate by itself to get a public key for encryption; and when the ARCOT credential-holder sends a signed transaction to a non-ARCOT enabled user, the X.509 certificate is provided without any ARCOT wrapping. Thus, earlier concerns over non-interoperability were allayed. ARCOT is looking into being FIPS-140 validated. Agencies were encouraged to contact ARCOT to get the details on their product offerings, at the discretion of the agency.

Funding:
Continuing to go after $7M for Fiscal Year 01. The House/Senate appropriations zeroed-out our funding. The Office of Management and Budget (OMB) perseverance restored

$3.5M in the appropriations conference committee. OMB is trying to get the other $3.5M restored. However, the entire appropriations bill is under veto threat (for unrelated reasons) so nothing is guaranteed.

The break-down of $7M is as follows: $1.5M goes to the Federal Bridge Certification Authority (FBCA), $.5M goes to the Policy Authority, $.5M goes to Treasury for funds management, and $4.5M goes to fund agencies to interoperate with the FBCA. If only $3.5M is obtained, then the latter two categories are reduced to about $200K and $1.3M respectively.

GPEA Digital Signature Guidance:
The guidance has been finalized. It was provided to OMB for transmission to NIST, where it will be issued as a "special publication".

Web Page:
The Steering Committee web page, which is undergoing a complete remodeling, is 90% complete. This website is ready to be accessed. The new URL is: "http://cioc-pki.treas.gov/". This new URL reflects our transition to the CIO Council, rather than the GITS Board. However, the old URL ("http://gits-sec.treas.gov/") is still active. We are currently in discussions to transport the website from a Treasury server to a GSA server. Details will follow.

ACES Update
Judy Spencer from GSA provided an update on ACES. Judy advised that the ACES Customer Advisory Board has decided to provide the Department of Veterans Affairs 100,000 of the "free-issuance" ACES certificates, and the Federal Emergency Management Agency 10,000 of those certificates. Agencies are encouraged to apply for the remaining 390,000 as soon as possible. (President Clinton received the first-two "free-issuance" certificates, provided by Digital Signature Trust, Inc., when he signed the E-Sign Bill S.761.) Judy also advised that she is researching whether ACES may be able to supply roaming solutions to agencies.

Discussion
To close out the discussions which had been held over the past two months on roaming solutions, Rich provided the following overview on different ways to implement a PKI, so that agencies can made informed decisions; this overview preceded a presentation by Entrust on roaming solutions.

a. Generating, storing and using keys on hardware token. This is the most secure and usually the most expensive approach. All cryptographic functions are performed on the token, and all keys are held encrypted on the token. If the tokens are smartcards, you need card-readers on all PCs.

b. Private key protected on hardware disk or floppy disk. This is the most widespread approach to-date. It offers better security than just PINs/Passwords, but since the signing or encryption events occur in computer memory, they can be attacked if the computer has

malicious code; further, if a miscreant can get the file in which the encrypted password is held, that file can be attacked (e.g., using a dictionary attack) endlessly in an attempt to discover the password (whereas a hardware token, after a certain number of failed attempts, will lock up). Nonetheless, this approach does offer mobility – the encrypted private key file can be transported on a floppy disk.

c. Roaming Servers. No copies of encrypted private key are maintained on floppy or hard disks, just stored on a central server, usually double encrypted (with a user password and a server symmetric key). To use the private key, the user needs to authenticate himself or herself to the roaming server, whereupon the encrypted private key is downloaded to the desktop, activated (in some cases) by a second password, and then used to make a signature or decrypt a document; thereafter, the private key is discarded from memory (its presence is ephemeral). Specific note: a roaming credential used in concert with a one-time-password (like RSA's Secure ID) provides better than one factor authentication and may be attractive to agencies who desire mobile credentials but want better protection than is afforded by a persistent password. If malicious code exists on a desktop, however, a copy of the private key could be obtained because the crypto operations are performed in memory rather than on a hardware token.

After this introduction, Chris Voice, Director, Product Management at Entrust, gave a presentation on roaming-solutions which included Entrust's offering, TruePass. (Rich noted that other vendors also offer roaming solutions, and encouraged agencies to talk to each PKI vendor about its specific offering if the agency desires a roaming solution.)</p>

Technical Working Group (TWG)
There will be a TWG on 10 August, from 9am to 4pm, at the USPTO (Crystal Park 1, 2011 Crystal Drive, Room 601b, Crystal City, VA).

Legal Policy Working Group (LPWG)
The Department of Justice (DOJ) is drafting a Memorandum of Agreement (MOA) between the FPKI Policy Authority (PA) and an applicant government agency for interoperability with the Federal Bridge Certification Authority (FBCA). This document will be provided to the FPKIPA for their review and approval after the Steering Committee has had an opportunity to review it.

Business Working Group (BWG)
BWG meetings will resume in the September timeframe. The BWG will be co-chaired by representatives from GSA and the three ACES contractors, ORC, AT&T, and DST.

Conclusion:
The meeting was adjourned at 03:00 P.M. The next meeting will be on 11 September, from 9:30am to 12:00pm, at GSA (same location).