Federal Public Key Infrastructure Policy Authority (FPKIPA)

Draft Minutes of the 8 January 2008 Meeting

USPS, 475 L'Enfant Plaza, SW, Washington, DC
Conference Room 2P316 (Inside 2P310)

A. AGENDA

1. Welcome / Introductions
2. Discussion / Vote on 11 December 2007 FPKIPA Minutes
3. Revocation of DoD Cross Certificate (ECA and DoD Interoperability Root CA)
4. FPKI Certificate Policy Working Group (CPWG) Report
   a. *Discuss 13 December 2007 CPWG Meeting*
   b. *Discuss 3 January 2008 CPWG Meeting*
5. FPKI Operational Authority (FPKI OA) Report – Cheryl Jenkins
   a. *Certificate Directory Status*
   b. *Key Rollover Status*
   c. *Interoperability Testing Status*
6. *Update on SSP and* SSPWG Activities
7. Final Meeting Items
   a. Other Topics: Federal Agencies Upgrade to 3647 RFC Format
   b. Proposed Agenda for 12 February 2008 FPKIPA Meeting
8. Adjourn Meeting

B. ATTENDANCE LIST

VOTING MEMBERS

The meeting began with a quorum of 14/15 (or 93.3%), where a two-thirds majority was required. This included three proxies. (GPO, SSA and USPTO).

We redacted contact information in the published FPKIPA minutes at the request of FPKIPA members. This information will be posted to a secure web site for FPKIPA members only at some point in the future. FPKIPA minutes already posted on the website have been redacted to remove POC information. FPKIPA members needing POC information on other members and participants should contact the Secretariat at Judith.fincher@enspier.com.

Organization	Name	Telephone
Department of Commerce (NIST)	Cooper, David	
Department of Defense	Mitchell, Debbie	
Department of Health & Human Services	Alterman, Dr. Peter	
Department of Homeland Security	Hagerling, Don	
Department of Justice	Morrison, Scott	
Department of State	McCloy, Mark A.	
Department of Treasury	ABSENT	
Drug Enforcement Administration (DEA CSOS)	Jewell, Chris	Teleconference
GPO – Proxy to HHS	Hannan, John--Proxy to HHS	
GSA	Temoshok, David	
NASA	DeYoung, Tice	Teleconference
Nuclear Regulatory Commission- NRC	Sulser, David	

Organization	Name	Telephone
SSA - Proxy to DoD	Mitchell, Eric--Proxy to DoD	
USPS	Stepongzi, Mark	
USPTO - Proxy to Commerce	Robinson, Quentin--Proxy to Commerce	

OBSERVERS

Organization	Name	Telephone
FPKI/FICC Support (Contractor--General Dynamics Information Technology)	Petrick, Brant	
FPKIPA Secretariat (Contractor -- Enspier Technologies/Protiviti Government Services)	Fincher, Judy	
DoD PKI PMO (contractor)	Ryan, George	
IdenTrust (vendor)	Young, Kenny	Teleconference
FPKI OA Technical Lead (Contractor—Enspier Technologies/Protiviti Government Services)	Brown, Wendy	
GSA (Attorney)	Cornell, John	Teleconference
FPKI OA/GSA (PM)	Jenkins, Cheryl	Teleconference
Wells Fargo	Drucker, Peri	Teleconference
MIT Lincoln Laboratory IT Security, ICS	Malabon, Mikiala	Teleconference
DoD (Attorney)	Russell, Shauna	
KPMG	Faut, Nathan	
FPKI/FICC/GSA	Spencer, Judith	
DoS (Contractor, ManTech)	Froehlich, Charles	

C. MEETING ACTIVITY

Agenda Item 1

Welcome / Introductions—Dr. Peter Alterman, Chair

The FPKIPA met at the USPS Headquarters Building located at 475 L'Enfant Plaza, SW, Washington, DC, in Conference Room 2P316 (inside 2P310). Dr. Peter Alterman, Chair, called the meeting to order at 9:38 a.m. with the attendee roll call. We wish to thank Mr. Mark Stepongzi of the USPS for finding us a meeting place upon very short notice and for hosting this meeting. Ms. Shauna Russell, the attorney for the DoD PKI PMO and George Ryan, a contractor who supports the DoD PKI PMO, participated in the discussion of Agenda Item 3.

Agenda Item 2

Discussion / Vote on 11 December 2007 FPKIPA Minutes—Judy Fincher

Ms. Fincher said she incorporated all comments received and distributed a redline version of the minutes to the FPKIPA five working days prior to the 8 January 2008 FPKIPA meeting. DoD (Debbie Mitchell) objected to voting on the minutes since she was unable to provide her comments due to the holidays.

ACTION: Debbie Mitchell will submit her comments on the 11 December 2007 FPKIPA minutes to the Secretariat this week. (Done)

ACTION: The Secretariat will incorporate DoD's comments on the 11 December 2007 FPKIPA minutes and initiate an e-vote this week.

Agenda Item 3

Revocation of DoD Cross Certificate (ECA and DoD Interoperability Root CA)—Dr. Peter Alterman, Debbie Mitchell, George Ryan, Shauna Russell, John Cornell, Judith Spencer, Dave Cooper, et al

Background

DoD has a large, widely deployed operational PKI that has a lot of legacy equipment and non-VISTA-compliant Microsoft operating systems, making it difficult for them to transition these sub-CAs to 2048-bit keys within the required timeframe.

For the past seven (7) years, the DoD has only provided a one-way cross-certificate to the FBCA cross-certified members (ECA). In July 2007 DoD cross certified a new Interoperability Root (IR) CA with the FBCA using a two-way certificate. To date, DoS (Charles Froehlich) says, the IR is a one-link chain that is not useful. Even the DoD PKI PMO does not have authorization to require the use or recognition of it, but someone within DoD must, as witnessed by JRF CTO 06-02.

Meeting Discussion

Dr. Alterman and Judith Spencer opened the topic discussion by providing background on the high-level negotiations that occurred between the DoD (Morris Hymes, Shauna Russell, Debbie Mitchell, and George Ryan) and the FPKIPA (Dr. Peter Alterman, Judith Spencer, Dave Cooper, John Cornell). The issue is that DoD is currently out of compliance with NIST SP 800-57 and NIST SP 800-78-1. This guidance stipulates that 1024 bit keys must be transitioned to 2048-bit keys no later than December 31, 2010, and the DoD is continuing to issue three-year certificates that would expire after that deadline.

In late December the DoD provided a copy of its “PKI Algorithm Transition Strategy” to the FPKIPA, but to date, this document has not been distributed.

ACTION: Judy Fincher will distribute the DoD's PKI Algorithm Transition Strategy to the FPKIPA listserv.

FPKIPA management feels the migration strategy is acceptable, but there is a “show stopper”. DoD is also insisting that they be given a waiver to continue to issue three year 1024 bit certificates until they are ready to transition to 2048 bit keys, estimated to occur by the end of 2008. And, if for some reason this migration is not viable, they would then elect to consider elliptical curve algorithms, which would push out the migration to a larger crypto key size even further, possibly putting at jeopardy the security of the entire FPKIA for the next five years or longer.

Ms. Mitchell said that DoD will not support 2048-bit keys for end entities until we have 128kb cards (Sept. 07).

Debbie Mitchell and George Ryan explained the reasons for DoD's approach.

1) DoD wants to use up its CAC (64k) card stock and the 2048-bit certificates will not fit on the CAC card. Issuing two-year certificates is a cost issue, Mr. Ryan said. Each card costs $8 and this amounts to an additive cost of between $8M -10M. Ms. Spencer pointed out that DoD could replace the certificates on the CAC at a later time. Mr. Ryan said that the DoD CP does not permit this. Ms. Spencer rejoined: "You're asking us to change our policy yet you refuse to change yours."
2) DoD needs to do application testing regarding the transition to 2048-bit keys, to ensure it does not destroy their world.

Under the above scenario, DoD would continue to have older CAs in operation for the 1Q2008, but the transition would be completed by no later than 1Q2013.

The FPKIPA has proposed that the DoD:

1) Issue two-year certificates so that the certificates expire by the end of 2010, or
2) Employ two new policy OIDS for all three-year certificates issued after January 1, 2008. This would allow the existing cross-certificate to stay in place.

Failing this, the FBCA could cross-certify DoD at C4 until they come back into compliance. The C4CP gives 1024-bit keys a longer life span than the FBCA CP.

Debbie Mitchell, assisted by Shauna Russell and George Ryan, presented the DoD point of view at the meeting. The options presented by the FPKIPA were not viable, she said, because:

1) DoD has gone on record many times that they cannot comply with section 6.1.5. This was laid out in our FIPS 201 plan, she said, and OMB granted DoD the status of being a "legacy agency." We could break things by not testing beforehand, she said. "We can't just flip a switch because the operational PKI testing is complicated and time-consuming, e.g., three months estimate.
2) DoD has met with the FPKIPA management (Dr. Alterman, Judith Spencer, John Cornell) and with NIST (Tim Polk and Dave Cooper) to explain the DoD position.
3) DoD issued a White Paper on November 30, 2007, showing the revised timelines, and received a response from FPKIPA on December 17, 2007.

Ms. Mitchell said that DoD considered the two options presented by the FPKIPA and added additional ones, including:

1) Cross-certify using existing policy OIDs that will expire no later than December 30, 2010
2) Issue a second cross-certification to distinguish the new certificates from the existing ones.

Dr. Alterman said that the DoD proposals described above violate FPKIPA Policy. The situation, Dr. Alterman said, is that our policy does not allow us to grant waivers. Section 6.1.5 of the FBCA CP is the “date certain requirement.”[1]

The FPKIPA does not have any “wiggle room, Dr. Alterman said, adding; “this is a binary situation.”

Debbie Mitchell requested that the FPKIPA consider changing its policy regarding waivers as a way forward out of this impasse.

Debbie Mitchell then presented Mr. Morris Hymes’s concern with downgrading to a C4 policy. The C4 does nothing to guarantee interoperability between the DoD and other cross-certified members and/or with Replying Parties, she said. The focus is on the cross-certificate; and the focus should be on interoperability, Mr. Hymes contends. He also is insisting that we test the viability of using 2048-bit keys in a test infrastructure. Furthermore, Mr. Hymes wants to let the CIO Council weigh in on this matter. Mr. Temoshok suggested that we go through OMB and through them to the CIO Council.

Ms. Spencer explained that the CIO Council delegated responsibility for the FPKI architecture, infrastructure and operations to the FPKIPA in 2000. Since that time, the FPKIPA has self-managed the policy and day-to-day operations through its Charter and By-Laws, she said. David Temoshok concurred, saying that resolving issues of non-compliance is within the purview of the Charter and By-Laws.

David Temoshok pointed out that DoD is in violation of NIST requirements, which the FPKIPA is not empowered to waive or modify.

Judith Spencer said that when the FBCA policy was written that NSA instructed the FPKIPA not to include waivers in its policy.

David Temoshok asked if the waiver proposal that DEA CSOS had put forth previously might not be a way out of this impasse. In their proposal to the CPWG, DEA CSOS proposed issuing 1024-bit certificates beyond December 31, 2007, with the understanding that these would be revoked before December 31, 2010.

[1] Section 6.1.5: (Excerpt) “CAs that generate certificates and CRLs under this policy shall use signature keys of at least 1024 bits for RSA or DSA, and at least 160 bits for ECDSA. Certificates that expire after 12/31/2010 shall be generated with at least 2048 bit RSA key, or at least 224 bits for ECDSA.

CAs that generate certificates and CRLs under this policy shall use SHA-1, SHA-224, SHA-256, SHA-384, or SHA-512 hash algorithm when generating digital signatures. Signatures on certificates and CRLs that are issued after 12/31/2010 shall be generated using, at a minimum, SHA-224.

Where implemented, CSSes shall sign responses using the same signature algorithm, key size, and hash algorithm used by the CA to sign CRLs.

End-entity certificates shall contain public keys that are at least 1024 bit for RSA, DSA, or Diffie-Hellman, or 160 bits for elliptic curve algorithms. The following special conditions also apply:

- End-entity certificates that include a keyUsage extension that only asserts the *digitalSignature* bit that expire on or after 12/31/2013 shall contain public keys that are at least 2048 bits for RSA or DSA, or 224 bits for elliptic curve algorithms.

- End-entity certificates that do not include a keyUsage extension or that include a keyUsage extension that asserts the *nonRepudiation*, *keyEncipherment*, *dataEncipherment*, or *keyAgreement* bit that expire on or after 12/31/2010 shall contain public keys that are at least 2048 bits for RSA or Diffie-Hellman, or 224 bits for elliptic curve algorithms.”

ACTION: Judith Spencer will draft a request for NIST to provide an opinion as to whether they could accept the proposed “DEA CSOS” waiver language.

Dave Cooper explained that the CPWG refused to grant the DEA CSOS a waiver. No one can predict what will happen in 2010, he said. Will these certificates actually go away?

Dr. Alterman summarized the situation from the perspective of the FPKIPA.

1) DoD is out of compliance with NIST requirements
2) The FPKIPA is required by its Charter and By-Laws to deal with the non-compliance of cross-certified members
3) The FPKIPA may vote to revoke a cross-certificate “for cause”
4) Our policy does not allow us to waive or delay requirements.

In short, we should reduce their level of assurance to C4 so that they can comply, Dr. Alterman said. Ms. Mitchell said that C4 “does nothing for interoperability.”

Tice DeYoung cited the case of NASA when it temporarily gave up its voting status and then came back in.

Dr. Alterman said that it is not a question of voting rights; DoD is a Charter Member and as such is entitled to a vote whether they have a PKI or not.

John Cornell reiterated the options: Either the FPKIPA has to change its policy or vote to revoke the DoD’s cross-certificate(s).

Tice DeYoung stated that while revoking the DoD certificate would work politically, how would that work operationally?

Wendy Brown explained that the DoD cross-certificates that were accidently revoked on December 31, 2007, will be re-issued in the near future. Dr. Alterman acknowledged that revoking the certificates without a formal vote by the FPKIPA was a mistake and that he should have checked the By-Laws before proceeding. He also said he had instructed the FPKI OA to re-instate the DoD cross certificates.

Shauna Russell then proposed that DoD consider requesting a DEA CSOS-type “waiver.”

Ms. Spencer asked why the DoD shouldn’t just issue two-year certificates “if you are convinced you can comply with 2010?” Shauna Russell explained that DoD had tried to do this for the military cadets and that the issue had been discussed at “high levels.” Issuing two-year certificates would have required us to write new software and track the certificates. “We can’t do this today,” she said.

David Temoshok and others expressed the concern that other legacy PKI agencies might also have a problem conforming to the 2048-bit requirement. Dr. Alterman took an informal “straw poll.”

- Scott Morrison (DoJ) said Justice will comply by going to two-year certificates in the internal PKI

- DoS CAs are already 2048-bit compliant and has begun issuing two-year certs to end users
- DOD CAs are issuing 1024-bit keys and will continue
- HHS is already 2048-bit compliant (via an SSP)
- NRC is issuing 1-year certificates at 1024 bits (via an SSP)
- USPS has not issued certificates yet

ACTION: Dr. Alterman will ask legacy PKI agencies how they are addressing the 2048-bit issue, e.g., by limiting certificate life, by having implemented 2048-bit keys before January 1, 2008, or other solution.

Judith Spencer reminded the FPKIPA that their upgrades of their CPs to 3647 RFC format are also overdue. She said the CPWG would perform a re-mapping of all non-compliant policies as they upgrade.

Tice DeYoung made a motion which he subsequently withdrew to make DoD comply with the FPKIPA policy re 2048-bit keys by the time of the next FPKIPA meeting (February 12, 2008).

Judith Spencer also made a motion --which was not voted on-- requiring the FPKIPA to get a formal opinion from NIST as to whether or not the FBCA Policy can be changed without violating the crypto key requirements in NIST 800-57.[2]

ACTION: Shauna Russell, Co-Chair of the DoD CPMWG, will get a formal opinion as to whether DoD can change its policy regarding 2010 and the three-year certificates. She will report on this activity at the February 12, 2008 FPKIPA meeting.

Several members spoke for and against modifying the FBCA CP to accommodate the DoD. Charles Froehlich said that C4 would get DoD continued participation in the FPKI Architecture (FPKIA), since any FPKI member can choose to trust another via a direct trust relationship.

Don Hagerling said we need DoD's continued participation because they have an established base of PKI applications. I want to embrace DoD and their continued participation in this effort, he said. He pointed out there are other agencies that do not comply with all NIST policies. If they have a solution that could be deployed in 90 days, we should not revoke them, he said.

Dr. Alterman: If we do anything official, it will be considered a waiver. I'm trying not to drill you into the ground with an auger of your own making, he said, addressing DoD.

Dave Cooper suggested a way forward: have DoD submit a FBCA CP Change Proposal and convince NIST that we will not have the same problem three years from now.

[2] Since the 8 January 2008 FPKIPA meeting, the FPKIPA obtained that opinion from NIST. DoD will submit a FBCA CP Change Proposal that would allow Entity CAs that have certificates with 1024-bit RSA to continue to be cross-certified with the FBCA until 12/31/2010 regardless of when the 1024-bit certificates expire. NIST (Tim Polk) is willing to assert that this does not violate SP 800-57 since Federal relying parties would not make use of the 1024-bit keys after 2010.

ACTION: Judith Spencer, Debbie Mitchell and Dave Cooper will collaborate on a FBCA CP Change Proposal to provide alternative language for satisfying 800-57 trust requirements.

Dr. Alterman said that if this issue is not resolved by the 12 February 2008 meeting, the options are 1) C4, 2) revoke.

Agenda Item 4

FPKI Certificate Policy Working Group (CPWG) Report—Dave Cooper

a. *Discuss 13 December 2007 CPWG Meeting*
b. *Discuss 3 January 2008 CPWG Meeting*

We did not discuss this item due to time pressures.

Agenda Item No. 5

FPKI Operational Authority (FPKI OA) Report —Cheryl Jenkins, Wendy Brown

a. Certificate Directory Status
b. Key Rollover Status
c. Interoperability Testing Status

We did not discuss this item due to time pressures.

Agenda Item No. 6

Update on SSP and SSPWG Activities

We did not discuss this item due to time pressures.

Agenda Item No. 7

Final Meeting Items

a. Other Topics: Federal Agencies Upgrade to 3647 RFC Format
b. Proposed Agenda for 12 February 2008 FPKIPA Meeting (to be held at the same location as today)
    i. Discuss/Vote on the 8 January 2008 FPKIPA Minutes
    ii. Briefing by Shauna Russell on the DoD Algorithm Transition Strategy Proposal
    iii. Results of Testing Environments Poll
    iv. Results of nextUpdate field Poll
    v. Results of Chairman's "straw polls" of FPKIPA cross-certified members

Agenda Item No. 8

Adjourn Meeting

Dr. Alterman adjourned the meeting at 11:55 a.m.

CURRENT ACTION ITEMS

No.	Action Statement	POC	Start Date	Target Date	Status
285	Judith Spencer and DoD will go off-line to discuss name uniqueness. She suspects there is name collision.	Judith Spencer, Debbie Mitchell	8 May 2007	22 May 2007	Open
303	The FPKIPA asked that Tim Polk prepare a written rationale for these changes, since the weakness of SHA-1 and 1024 bit keys is of great concern to many members and extending their lifetime may increase the threat that these algorithms be compromised	Tim Polk	10 July 2007	14 August 2007	Open
315	Cheryl Jenkins will generate the SAFE Interoperability Test Report once it is determined that all remaining issues have been resolved.	Cheryl Jenkins	9 Oct. 2007	19 Oct. 2007	Open
315	Dr. Alterman and John Cornell will incorporate language into the FPKIPA audit Cook Book." This language was provided by Noel Nazario of KPMG and says that if customers set up the terms of their Web Trust audits appropriately, the Web Trust audit would satisfy all our requirements.	Dr. Alterman, John Cornell	9 Oct. 2007	13 Nov. 2007	Open
316	Judith Spencer said we should post an explanation of the purpose of the C4CP to the FPKIPA website, explaining that the FPKIPA needs this policy for those entities who cannot meet Federal Bridge cross-certification requirements, but who need an E-Authentication Level 2 credential.	??	13 Nov. 2007	26 Nov. 2007	Open
327	Cheryl Jenkins will send the annotated Implementation Plan to Judy Fincher for distribution to all cross-certified members of the FPKIPA.	Cheryl Jenkins	11 Dec. 2007	January 2008	Open
329	Judy Fincher will distribute the DoD's PKI Algorithm Transition Strategy to the FPKIPA listserv.	Judy Fincher	8 Jan. 2008	15 Jan. 2008	Open
330	Judith Spencer will draft a request for NIST to provide an opinion as to whether they could accept the proposed "DEA CSOS" waiver language.	Judith Spencer	8 Jan. 2008	15 Jan. 2008	Open

No.	Action Statement	POC	Start Date	Target Date	Status
331	Dr. Alterman will ask legacy PKI agencies how they are addressing the 2048-bit issue, e.g., by limiting certificate life, by having implemented 2048-bit keys before January 1, 2008, or other solution.	Dr. Alterman	8 Jan. 2008	15 Jan. 2008	Open
332	Shauna Russell, Co-Chair of the DoD CPMWG, will get a formal opinion as to whether DoD can change its policy regarding 2010 and the three-year certificates. She will report on this activity at the February 12, 2008 FPKIPA meeting.	Shauna Russell	8 Jan. 2008	12 Feb. 2008	Open