GSA Office of General Counsel

May 15, 2012

MEMORANDUM FOR DEBORAH GALLAGHER
CHAIR, FEDERAL PKI POLICY AUTHORITY

FROM: JOHN E. CORNELL
SENIOR ASSISTANT GENERAL COUNSEL
PERSONAL PROPERTY DIVISION (LP)

Digitally signed by JOHN CORNELL
Date: 2012.05.15 09:16:41 -04'00'

SUBJECT: Review of Federal PKI Auditor Letter

As requested, I have reviewed the Federal PKI Auditor Letter dated 28 February 2012.. My findings are as follows:

Audit Guidance	Findings
Identity of the Auditor and the individuals performing the audit	The auditor is Slandala, the individual is James Jung.
Competence of the Auditor to perform audits	The auditor is deemed competent.
Experience of the individuals performing the audit in auditing PKI systems	The individual meets the experience requirements of the CP.
Relationship of the Auditor to the entity that owns the PKI being audited. This relationship must clearly demonstrate the independence of the auditor from the entity operating or managing the PKI.	Outside auditor, deemed independent.
The date the audit was performed.	January 2012
Whether a particular methodology was used, and if so, what methodology.	Requirements decomposition methodology used.
Which documents were reviewed as a part of the audit, including document dates and version numbers.	The CP and CPS documents examined are set forth in the audit letter.
an audit summary is prepared, signed by the auditor	Requirement met.
State that the operations of the entity PKI's Principal CA were evaluated for	Requirement met

U.S. General Services Administration
1725 First Street, NE– Mail Stop LP
Washington, DC 20417
202-501-1598 (ph) 202-501-0583 (fax)
john.cornell@gsa.gov

conformance to the requirements of its CPS.	
Report the findings of the evaluation of operational conformance to the Principal CA CPS.	10 requirements found not to comply.
State that the entity PKI's Principal CA CPS was evaluated for conformance to the entity PKI's CP.	Requirement met.
Report the findings of the evaluation of the Principal CA CPS conformance to the entity PKI CP.	17 gaps found for FBCA and Common, 16 gaps found for E-gov.
For PKIs with multiple CAs, state whether audit reports showing compliance were on file for any additional CA components of the entity PKI	N/A (this report covers all CAs used by FPKI)
State that the operations of the Entity PKI's Principal CA were evaluated for conformance to the requirements of all current cross-certification MOAs executed by the Entity PKI with other entities.	Requirement met.
Report the findings of the evaluation of the Principal CA CPS conformance to the requirements of all current cross-certification MOAs executed by the Entity PKI.	Operations were in compliance with all MOAs, although the auditor noted that several of the MOAs were "very old and could be updated."

The auditor's letter was well done, but as noted above, there are gaps between the applicable CP and CPS documents, as well as findings that ten requirements of the CPS were not met in the operations of the CA(s).

Subsequent to receipt of the audit, the CP/CPS irregularities have been resolved. The remaining open issues:

1) The Policy Authority authorized issuance of two SHA-1 certificates after 12/31/2010, notwithstanding the fact that Common Policy doesn't allow this. These certificates expire 12/31/2013. This can be resolved in two ways – either ignore the issue until the certificates expire, or amend the policy to allow these two certificates to exist.

2) The e-government CA does not have subscriber agreements on file. Subscriber agreements have been drafted and will be forwarded to the subscribers for signature.

All of the others issues flagged in the audit have been resolved.

I recommend that the CPWG accept the audit as satisfying the CP requirements for a compliance audit and forward the matter of the CP change to the FPKI-PA.