



Member – Information Systems Audit and Control Association
Member – International Association of Privacy Professionals
Accredited Kantara Initiative Assessor

November 9, 2010

Ms. Cheryl Jenkins
Federal PKI Management Authority Program Manager
U.S. General Services Administration
1800 F Street, NW
Washington, DC 20405

Re: Federal PKI Management Authority Fiscal Year 2010 Public Key Infrastructure Lead Auditor's Compliance Report, dated October 29, 2010

Subject: Lead Auditor's PKI Compliance Opinion

Dear Ms. Jenkins:

The U.S. General Services Administration (GSA) Federal Public Key Infrastructure (FPKI) Management Authority (MA) requested an “*initial day*” compliance audit be conducted on the FPKIMA certification authorities (CA). This compliance audit was initiated to independently verify if the FPKIMA CPS complied with its applicable governing document, the Federal Bridge CA, Federal Common Policy, eGovernance, and C4CA certificate policies (CP(s)) and any signed memorandums of agreement in force for this PKI domain.

The FPKI architecture is a multi-policy domain with six self-signed root certification authorities (CA) in hierarchical position level 0. The FPKIMA CA(s) have been assigned regional context (X.501) syntax distinguished name (DN) embedded into the applicable self-signed digital certificates as follows:

- c=US, o=U.S. Government, ou=FPKI, cn=Federal Bridge CA;
- c=US, o=U.S. Government, ou=FPKI, cn=Federal Common Policy CA;
- c=US, o=U.S. Government, ou=FPKI, cn=eGovernance CSP1 CA;
- c=US, o=U.S. Government, ou=FPKI, cn=eGovernance CSP2 CA;
- c=US, o=U.S. Government, ou=FPKI, cn=eGovernance App CA; and
- c=US, o=U.S. Government, ou=FPKI, cn=C4 CA.

The lead auditor, Mr. Brian Dilley, primarily performs PKI auditing as a continual business service. He is a Certified Information Systems Auditor (CISA), a professional Certified in the Governance of Enterprise IT (CGEIT) in good standing with the Information Systems Audit and Control Association, and a Certified Information Privacy Professional (CIPP) in good standing with the International Association of Privacy Professionals. In addition, Mr. Dilley is the world's first accredited Kantara Initiative Assessor for global identity management and has more than 27 years of cumulative enterprise IT and specialized PKI domain experience such as:

Federal Bridge Certification Authority (FBCA) Project Manager, Chief PKI Architect, Policy Mapping Expert, Mozilla Firefox Auditor, Master User, System Administrator, Internal PKI Auditor, CP/Certification Practices Statement (CPS) author, Navy Cryptographer, CMS Custodian, Top-Secret Control Officer, Nuclear Quality Assurance Inspector, Identity Management SME, and External PKI Auditor for many major PKI and IT implementations.

The independence of the eValid8[®] audit team was established by the following criterion:

- That only auditing services were procured from this team,
- The audit team does not hold or is not assigned to any trusted roles within the PKI environment, and
- The audit team did not write any controls exhibited within the CP or CPS.

Therefore, the eValid8[®] audit team was determined to be an independent third party and was engaged to conduct a PKI compliance audit on the IRCA.

To determine the audit scope, the audit team utilized the assertions identified in the FPKI Policy Authority "Triennial Audit" document for initial day audits. For a list of audit artifacts, refer to this letter's *Appendix – Reference Audit Artifacts*. In addition, a lead auditor's opinion compliance letter is issued in accordance with U.S. Federal PKI auditor guidelines for reporting. eValid8[®] is the exclusive owner of the *eValidated*[®] TrustedCA/TrustedRA registered trade and service marks which were the audit methodology utilized for this audit engagement.

The audit team conducted an "initial" PKI compliance audit of the fully configured production FPKIMA CAs to validate the conformity of the FPKIMA CPSs¹ to the applicable FPKIMA CP. The compliance stated audited period was September 2, 2010 through September 30, 2010. This audit evaluated the management assertions² contained within the applicable FPKIMA certificate policies³ in effect during the stated audited period to verify that sound provisioning guidelines for the proper issuance of digital certificates were adhered to as defined.

The lead auditor hereby provides the following executive conformity summary of the FPKIMA CAs audit findings based on the lead auditor's detailed report prepared by eValid8[®]. The *eValidated*[®] compliance ratings assigned by the lead auditor are based upon three facilities visited (primary/backup hosting, and archive) with 12 artifacts being reviewed. Of the 56 Federal PKI CP(s) statements associated with FPKIPA initial audit parameters, the lead auditor declares

¹ United States Federal PKI Architecture X.509 Certification Practice Statement, version 3.2, dated July 19, 2010

² eValid8[®] Corporation letter, Ms. Cheryl Jenkins, FPKIMA Program Manager, U.S. General Service Administration, Subject: Management Assertions dated September 7, 2010

³ X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA), Version 2.17, June 10, 2010; X.509 Certificate Policy For The U.S. Federal PKI Common Policy Framework, Version 3647 - 1.10, dated April 8, 2010; X.509 Certificate Policy for the E-Governance Certification Authorities, Version 1.5, dated August 16, 2010; Citizen and Commerce Class Common Certificate Policy, Version 2.2, dated August 25, 2010

the initial *eValidated*[®] compliance determinations, before client resolution of identified concerns, to be:

- 22 CPS practices were deemed as *Satisfy*;
- 15 CPS practices were deemed as *Satisfy – Recommend*;
- 9 CPS practices were deemed as *Does Not Satisfy*;
- 3 CPS practices were deemed as *Missing*;
- 4 CP assertions were deemed *Not Applicable*;
- 2 CP assertions were deemed as *Duplicate*; and
- 1 CP assertion was deemed as *Informative*.

This initial review revealed 12 conformity concerns, resulting in an initial *eValidated*[®] compliance audit score of 78.57%.

For this audit the lead auditor requested the FPKIMA provide evidence of previous-year PKI auditing for the FPKIMA CAs. This request is not applicable due to the “initial” creation of these new CAs. At this point in time the above listed FPKIMA CA(s) have not issued any cross certificates to any other PKI domain entities.

By the submittal of new CP and CPS change proposal language, configuration files, and by submitting configuration files, documents, and other artifacts that were then reviewed and verified by the lead auditor, it is noted that the Federal PKI MA corrected 10 of the 12 initial audit concerns. Of the 56 Federal PKI CP(s) statements associated with initial day audit parameters, the lead auditor declares the final *eValidated*[®] compliance determinations to be:

- 31 CPS practices were deemed as *Satisfy*;
- 18 CPS practices were deemed as *Satisfy – Recommend*;
- 4 CP assertions were deemed *Not Applicable*;
- 2 CP assertions were deemed as *Duplicate*; and
- 1 CP assertion was deemed as *Informative*.

This final review revealed two conformity concerns, resulting in a final *eValidated*[®] audit score of 100%.

These FPKIMA CA(s) are new instances of CA(s) within the Federal PKI domain. In accordance with the “audit cookbook” provided by the FPKIPA the following additional audit reporting criteria for these new CA(s) is as follows:

1. State which procedures have been performed using the operational system and could be fully evaluated for conformance to the requirements of the entity PKI CPS;
 - a. Only those “initial day” audit criterion as defined within the Federal PKI “triennial” audit document were addressed and evaluated for this audit.
2. State which procedures have not been performed on the operational system and were evaluated for conformance to the requirements of the entity PKI CPS, but only with respect to training and procedures;
 - a. Only 56 of the 453 controls or assertions contained with the applicable FPKI certificate policy were addressed by an “initial day” audit. The other CP

- assertions were not defined within the audit charter and therefore were not verified for the new FPKIMA CA(s) under this initial day audit.
- b. The FPKIMA has a technical operations manual to address trusted role functions and tasks. The operations manual does not address policy authority or managerial operations. In addition, the FPKIMA operations manual is not aligned nor conforms to the IETF RFC 3647 framework for CPS documents. However, this operations manual is utilized by all trusted roles and is used for in-house training and awareness to operational capabilities.
3. State that the entity PKI(s) CPS was evaluated for conformance to the supported certificate policies;
 - a. Only those “initial day” audit CP criteria as defined within the Federal PKI “triennial” audit document were addressed for this audit. The FPKIMA CPS statements related to the FPKIPA “initial day” CP assertions were validated for compliance of the CPS practice to the supported CP assertion.
 - b. The lead auditor reviewed the applicable CP to the applicable CPS and both documents conform to the IETF RFC 3647 format for CP and CPS framework. Although not all CP assertions for a full compliance audit were verified during this initial day audit, the remaining CPS section headers and items were compared to the CP section headers and items and were found to be compliant with the above referenced RFC.

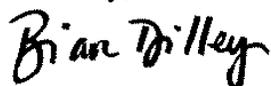
It is the lead auditor’s “*unqualified opinion*” that the six FPKIMA CAs with the above identified distinguished names, and the FPKIMA has satisfied him, with reasonable assurance, that effective control practices within the applicable CPS are in place that ensure the FPKIMA CPS(s) conform to the 56 FPKIMA CP(s) initial day audit criterion. It is strongly recommended by the lead auditor that any new activities employed or implemented by these new CA(s) be fully compliant with all aspects of the FPKIP CP, applicable MOA or cross-certificate agreement, and other government mandates for IT systems, such as OMB M04-04 for logical and e-authentication accesses.

The National Institute of Standards and Technology assigned the following IETF notation arc for FPKIMA policies as listed below:

POLICY	OBJECT IDENTIFIER
csor-certpolicy OBJECT IDENTIFIER	::= { 2 16 840 1 101 3 2 1 }
fbca-policies OBJECT IDENTIFIER	::= { csor-certpolicy 3 }
id-fpki-certpcy-rudimentaryAssurance	::= { fbca-policies 1 }
id-fpki-certpcy-basicAssurance	::= { fbca-policies 2 }
id-fpki-certpcy-mediumAssurance	::= { fbca-policies 3 }
id-fpki-certpcy-mediumHardware	::= { fbca-policies 12 }
id-fpki-certpcy-medium-CBP	::={ fbca-policies 14 }
id-fpki-certpcy-mediumHW-CBP	::={ fbca-policies 15 }
id-fpki-certpcy-highAssurance	::= { fbca-policies 4 }
id-fpki-certpcy-pivi-hardware	::={ fbca-policies 18 }
id-fpki-certpcy-pivi-cardAuth	::={ fbca-policies 19 }

id-fpki-certpcy-pivi-contentSigning	::= { fbca-policies 20 }
id-fpki-common-policy	::= {2 16 840 1 101 3 2 1 3 6}
id-fpki-common-hardware	::= {2 16 840 1 101 3 2 1 3 7}
id-fpki-common-devices	::= {2 16 840 1 101 3 2 1 3 8}
id-fpki-common-authentication	::= {2 16 840 1 101 3 2 1 3 13}
id-fpki-common-High	::= {2 16 840 1 101 3 2 1 3 16}
id-fpki-common-cardAuth	::= {2 16 840 1 101 3 2 1 3 17}
id-eGov-Level1	::= {2 16 840 1 101 3 2 1 3 9}
id-eGov-Level2	::= {2 16 840 1 101 3 2 1 3 10}
id-eGov-Applications	::= {2 16 840 1 101 3 2 1 3 11}
citizen-and-commerce-approved	::= 2.16.840.1.101.3.2.1.14.2

Sincerely,



Brian Dilley CISA / CGEIT / CIPP / Accredited Kantara Assessor
Lead Auditor
(443) 955.9885

Appendix – Reference Audit Artifacts

1. X.509 Certificate Policy For The U.S. Federal PKI Common Policy Framework, Version 3647 - 1.11, dated August 16, 2010
2. United States Federal PKI Architecture X.509 Certification Practice Statement, Version 3.2, dated 19 July 2010
3. United States Federal PKI Architecture X.509 Certification Practice Statement, Version 3.3, dated 29 September 2010
4. Federal Public Key Infrastructure Management Authority (FPKI MA) Operations Manual, Version 2.0.1, dated August 29, 2010
5. Terremark North America, Inc. Colocation Services, Independent Service Auditor's Report on Controls Placed in Operation and Tests of Operating Effectiveness, For the Period of January 1, 2009, to November 15, 2009, by SAS70 Solutions Certified Public Accountants
6. Federal PKI UniCERT Certification Authority Initialization and Root Key Signing Procedures Key Generation Ceremony Script, Version 2.0, dated September 2, 2010
7. Federal Public Key Infrastructure Management Authority (FPKI MA) Operations Manual, Version 2.0.1, dated August 29, 2010
8. X.509v2 Certificate Revocation Lists
 - a. Federal Bridge Certification Authority
9. X.509v3 Digital Certificates
 - a. Federal Bridge Certification Authority
 - b. Federal Common Policy Certification Authority
 - c. eGovernance CSP1 CA
 - d. eGovernance CSP2 CA
 - e. eGovernance App CA
 - f. C4 CA