U.S. GOVERNMENT PRINTING OFFICE
OFFICE OF INSPECTOR GENERAL

ASSESSMENT REPORT
10-09

WEBTRUST ASSESSMENT OF GPO'S PUBLIC KEY INFRASTRUCTURE CERTIFICATION AUTHORITY – ATTESTATION REPORT

September 20, 2010

MEMORANDUM

U.S. GOVERNMENT PRINTING OFFICE

OFFICE OF INSPECTOR GENERAL

Date

September 20, 2010

To

Chief Information Officer

From

Assistant Inspector General for Audits and Inspections

Subject

WebTrust Assessment of GPO's Public Key Infrastructure Certification Authority – Attestation Report
Report Number 10-09

The Government Printing Office (GPO) Office of Inspector General (OIG) has completed the WebTrust assessment of GPO's Public Key Infrastructure (PKI) Certification Authority (CA) for 2010. The purpose of the assessment was to determine whether GPO's management assertion related to the adequacy and effectiveness of controls over its CA operations, is in all material respects fairly stated. To conduct the assessment, the OIG contracted with Ernst and Young LLP (E&Y), an independent public accounting firm licensed by the American Institute of Certified Public Accountants (AICPA) to provide WebTrust assurance services. Management of the GPO Certification Authority should be commended for once again passing this rigorous assessment.

Background and Objectives

GPO has implemented a PKI to support its "born digital and published to the web" methodology to meet GPO customer expectations of being official and authentic. The GPO PKI also directly supports GPO's mission related to electronic information dissemination and e-Government. The GPO CA issues, signs and manages the public key certificates in secure facilities based in Washington, D.C. The GPO PKI is cross-certified with the Federal Bridge Certificate Authority (FBCA). FBCA certification provisions require the GPO PKI to undergo a compliance review on an annual basis.[1] To satisfy this compliance requirement, the OIG tasked E&Y to conduct a WebTrust

[1] Compliance review requirements can be found at (http://www.idmanagement.gov/fpkipa/documents/audit_guidance.pdf)

assessment of its CA. The assessment was conducted in accordance with the AICPA's WebTrust Principles and Criteria for Certificate Authorities and Statement on Standards for Attestation Engagements (SSAE) Number 10. The assessment represents an evaluation of whether GPO's assertion related to the adequacy and effectiveness of controls over its CA operations is fairly stated based on underlying principles and evaluation criteria.

The scope of the assessment included the following entities involved with operating the GPO CA:

- CA Policies and Procedures;
- Registration Authorities;
- Certification Authorities and Repository; and
- CA Supporting Systems, Databases and PKI facilities.

The assessment also measured the GPO CA's compliance with reporting requirements of the Federal Public Key Infrastructure Policy Authority (FPKIPA).

As a result of work performed, E&Y issued an Attestation Report (enclosure) which expresses their unqualified opinion that GPO management's assertion related to the adequacy and effectiveness of controls over its CA operations is, in all material respects, fairly stated based on the AICPA WebTrust for Certification Authorities Criteria. Additionally, E&Y issued a Letter of Supplementary Information to address additional FPKIPA reporting requirements. E&Y provided the means to display the report electronically as appropriate with access via GPO's designated website through an E&Y branded WebTrust seal for a period of 12 calendar months from issuance and for a longer period upon E&Y's prior written consent. GPO should implement the seal as a hyperlink to the assertion and attestation report maintained on the AICPA's secure server, to a Universal Resource Locator provided by E&Y. GPO may also, at its discretion, provide a brief narrative and hyperlinks to the assertion and report on the AICPA server, as approved by E&Y. GPO can display the seal on one or more web pages within the noted GPO domains at its discretion. The seal and the report may not be used on websites or in other ways not expressly permitted by Ernst and Young.

This Attestation Report covers the period July 1, 2009 through June 30, 2010. Upon direction by the OIG, E&Y will perform future examination procedures to support the issuance of updated reports. The timing of such updates depends on factors such as the amount of change that has occurred since the last update. Subsequent reports must cover a continuous representation period (i.e. commencing either on the beginning or ending date of the prior report) of up to 12 months.

In the event of material changes to GPO's CA system, additional assessment procedures may be required to determine whether GPO continues to meet the WebTrust for CA criteria and to issue an updated assessment report. If additional assessment procedures are required but not performed, E&Y has the option of declaring that the GPO no longer meets the WebTrust for CA criteria and GPO would forfeit the right to display the electronic WebTrust Seal. **Therefore, please notify the OIG in advance in the event that GPO makes material changes to its CA system, including changes to controls, information handling practices, or disclosures; in the manner in which GPO complies with the WebTrust for CA criteria, in the nature of the products, information, or services offered; or changes in the systems used to support the GPO CA.**

The report contains no recommendations and therefore we are not requesting a management response. The final report distribution is in the Appendix to this report. If you have any questions concerning the report or the assessment process, please contact Mr. Brent Melson, Deputy Assistant Inspector General for Audits and Inspections at (202) 512-2037, or myself at (202) 512-2009.

Kevin J. Carson

Kevin J. Carson
Assistant Inspector General for Audits and Inspections

Enclosure

Ernst & Young
8484 Westpark Drive
McLean, Virginia 22102

Tel: + 1 703 747 1000
www.ey.com

Report of Independent Accountants

To the Inspector General of the United States Government Printing Office and the Management of the United States Government Printing Office Certification Authority (GPO-CA):

We have examined the assertion by the management of the US Government Printing Office (GPO) that in providing its Certification Authority (CA) services known as GPO Public Key Infrastructure Certification Authority (GPO-CA) in Washington, DC for the Root CA: GPO-CA during the period from July 1, 2009 through June 30, 2010, GPO-CA has:

- Disclosed its key and certificate lifecycle management business and information privacy practices in its Certificate Practices Statement and provided such services in accordance with its disclosed practices:
- Maintained effective controls to provide reasonable assurance that:
  - Subscriber information was properly authenticated (for the registration activities performed by GPO-CA);
  - The integrity of keys and certificates it managed was established and protected throughout their lifecycles;
  - Subscriber and relying party information was restricted to authorized individuals and protected from uses not specified in the CA's business practices disclosure;
  - The continuity of key and certificate lifecycle management operations was maintained; and
  - CA systems development, maintenance and operations were properly authorized and performed to maintain CA systems integrity

  based on the AICPA/CICA WebTrust for Certification Authorities Criteria.

GPO-CA management is responsible for its assertion. Our responsibility is to express an opinion on management's assertion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants, and accordingly, included (1) obtaining an understanding of GPO-CA's key and certificate lifecycle management business and information privacy practices and its controls over key and certificate integrity, over the authenticity and privacy of subscriber and relying party information, over the continuity of key and certificate lifecycle management operations, and over development, maintenance and operation of systems integrity; (2) selectively testing transactions executed in accordance with disclosed key and certificate lifecycle management business and information privacy practices; (3) testing and

evaluating the operating effectiveness of the controls; and (4) performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

Because of inherent limitations in controls, errors or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that the validity of such conclusions may be altered because of changes made to the system or controls, the failure to make needed changes to the system or controls, or deterioration in the degree of effectiveness of the controls.

In our opinion, for the period from July 1, 2009 through June 30, 2010, GPO-CA management's assertion, as set forth in the first paragraph, is fairly stated, in all material respects, based on the AICPA/CICA WebTrust for Certification Authorities criteria.

The WebTrust seal of assurance for certification authorities on GPO-CA's website constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.

The relative effectiveness and significance of specific controls at GPO-CA and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other factors present at individual subscriber and relying party locations. We have performed no procedures to evaluate the effectiveness of controls at individual subscriber and relying party locations.

This report does not include any representation as to the quality of GPO-CA's services beyond those covered by the WebTrust for Certification Authorities Criteria, nor the suitability of any of GPO-CA's services for any customer's intended purpose.

Ernst + Young LLP

August 30, 2010

Ernst & Young
8484 Westpark Drive
McLean, Virginia 22102

Tel: + 1 703 747 1000
www.ey.com

Letter of Supplementary Information

To the Inspector General of the United States Government Printing Office and the Management of the United States Government Printing Office Certification Authority (GPO-CA):

This letter provides supplementary information to the examination performed by Ernst & Young LLP of the assertion by the management of the GPO-CA regarding the certification authority services it provides at http://www.gpo.gov/projects/pki.htm.

Management's assertions were based on the American Institute of Certified Public Accountants (AICPA)/Canadian Institute of Chartered Accountants WebTrust for Certification Authorities criteria. GPO-CA's management was responsible for its assertion. Our responsibility was to express an opinion on management's assertion based on our examination.

Our examination was conducted in accordance with attestation standards established by the AICPA and, accordingly, included examining, on a test basis, evidence about GPO's compliance with those requirements and performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion. Our examination does not provide a legal determination on GPO-CA's compliance with specified requirements.

The audit period for this examination was from July 1, 2009 through June 30, 2010. Our examination was performed between May 26, 2010 and August 14, 2010.

We examined the Certificate Policy (CP) for the GPO-CA version 1.3.1, dated August 17, 2009, and the Certification Practices Statements (CPS) for the GPO Principal Certification Authority (GPO-PCA) version 1.7, dated March 14, 2009. Multiple Root CAs were not in operation at GPO-CA.

Our examination included, through our testing of management's assertion, the evaluation of GPO-CA's operations for conformance to the requirements of its CPS and the evaluation of GPO-CA's operations for conformance to the requirements of all current cross-certification Memorandum of Agreements (MOAs) executed by the GPO-CA with other entities. In our Report of Independent Accountants dated August 14, 2010, we reported that management's assertion was fairly stated in all material respects.

ERNST & YOUNG

We have compared the CPS for the GPO-PCA version 1.7, dated March 14, 2009, for conformance to the CP for the GPO-CA version 1.3.1, dated August 17, 2009. We found, in all material respects, that the GPO-PCA CPS is in conformance with GPO-CA CP.

We are independent of the GPO for the professional engagement period as required by the AICPA Professional Standards.

Ernst & Young LLP

August 30, 2010

Ernst & Young
8484 Westpark Drive
McLean, Virginia 22102

Tel: + 1 703 747 1000
www.ey.com

Summary of Matters Related to Project Personnel Provided by Ernst & Young LLP

To the Inspector General of the United States Government Printing Office and the Management of the United States Government Printing Office Certification Authority (GPO-CA):

The GPO Office of Inspector General (OIG) has asked Ernst & Young LLP (EY or we) to provide certain information to assist in its efforts to provide the Federal Public Key Infrastructure Policy Authority (FPKIPA) with information about the individuals who performed work as part of the WebTrust for Certification Authority (WTCA) examination services; these services are performed in accordance with relevant American Institute of Certified Public Accountants (AICPA) standards. The FPKIPA sets policy governing operation of the U.S. Federal PKI Infrastructure, composed of: the Federal Bridge Certification Authority (FBCA); the Federal Common Policy Framework Certification Authority (CPFCA); the Citizen and Commerce Class Common Certification Authority (C4CA) and the E-Governance Certification Authority. EY makes no representation regarding the sufficiency of this information for the purposes for which this information was requested. That responsibility rests solely with the FPKIPA.

Educational Level and Professional Experience

Client serving personnel (Professionals) EY has provided to the Agency have received a degree from an accredited college or university (or its equivalent if the individual was educated outside of the United States). Certain individuals may also have advanced degrees. The majority of Professionals provided to the Agency are part of EY's Advisory Services (AS) service line. AS focuses its recruiting efforts on candidates with information technology, accounting, finance and other business-related degrees. Hiring activities and types of Professionals hired into each EY service line, including Assurance and Tax, are generally the same as similar service lines and personnel of Deloitte & Touche, PricewaterhouseCoopers and KPMG (who along with EY, are the Big Four).

The experience levels of Professionals provided will vary based upon various factors including age and length of time the individual has worked since receiving their degree. The amount of professional experience of Professionals may not solely be related to a person's employment period with EY, as EY normally hires a combination of experienced Professionals and Professionals who recently graduated from a college or university. In most cases, the experience level within a rank classification of EY Professionals is generally the same as the other Big Four.

Methodologies, Policies and Procedures

EY Professionals carrying out WTCA examinations are required to comply with policies and procedures within the EY Advisory Global Practice Manual and related methodologies. In those cases where we do not perform work directly under the supervision and responsibility of Agency personnel as part of an engagement to provide loan staff, and we provide management with our

findings and recommendations in those areas where we observe internal controls that, in our view, could be improved, the Advisory Global Practice Manual requires the work and any reports or deliverables to be in accordance with the Statement on Standards for Consulting Services (CS100) of the AICPA. The initial adoption of, and any subsequent changes in, policies and procedures have been reviewed and approved by EY's Professional Practice group.

Professional Certification and Continuing Education

EY encourages its Professionals to obtain a professional certification. In certain service lines, obtaining a professional certification is a requirement for promotion. Individuals in AS are encouraged to obtain a professional certification, but it is not a requirement of employment or advancement. AS' more experienced Professionals (which we refer to as managers, senior managers, executive directors, principals or partners) usually have a professional certification and some may have more than one certification. In the AS service line, the most common certifications are Certified Public Accountant (CPA) (or its equivalent in other countries), Certified Internal Auditor (CIA) as recognized by the Institute of Internal Auditors, Certified Information Systems Auditor (CISA) as recognized by the Information Systems Audit and Control Association, or Certified Management Accountant (CMA) as recognized by the Institute of Management Accountants.

The continuing professional education requirements of the SEC (Securities and Exchange Commission) Practice Section of the AICPA Division for CPA firms are the foundation of EY's professional development policy. The policy applies to all professionals and Government Accountability Office (GAO) Guidance, as confirmed in consultation with GAO personnel, suggests that staff and those individuals not managing an engagement subject to Government Auditing Standards (GAS) may generally satisfy the Government Auditing Standards (Yellow Book) 24 hour CPE requirement through completion of the firm's core training because significant portions of core training content involve auditing under AICPA standards and AICPA standards are incorporated into GAS. As a subset of the 24 hour GAS requirement, our firm has a governmental audit continuing education policy that applies to each individual acting as partner in charge, the independent reviewer, and each individual managing a governmental audit or attestation engagement. An individual's professional development principally occurs through formal learning and on-the-job training. Participation in formal education programs (including self-study programs and meetings organized at least in part for educational purposes) is intended to supplement on-the-job training and other learning activities.

Participation in professional development programs is measured in units of continuing professional education (CPE) credit hours earned in our educational year. EY's educational year is July 1 through June 30. The EY policy for compliance is as follows:

- Commencing with the first full educational year of employment, each professional must obtain at least 20 CPE credit hours each year and at least 120 CPE credit hours during the most recent three-year period.
- Professionals who were not employed during the entire most recent educational year are not required to earn continuing professional education credits in that year.

ERNST & YOUNG

- Professionals who were employed during the entire most recent educational year, but not during the entire most recent two educational years, are required to have participated in at least 20 hours of qualifying continuing professional education during the most recent educational year.

- Professionals who were employed during the entire most recent two educational years, but not during the entire most recent three educational years, are required to have participated in at least 20 hours of qualifying continuing professional education during each of the two most recent educational years.

Professionals who hold a professional designation or certification other than the CPA certification (e.g., CIA, attorney at law, CISA, CMA) may be subject to continuing education requirements as part of that designation or certification. Completion of courses to meet these requirements may be used to meet the firm's CPE requirements as long as the courses also meet the requirements of the AICPA's SEC Practice Section.

Experience Auditing PKI Systems

The EY executive team assigned to the GPO project has experience in performing audits and implementation of PKI systems and IT security. In addition, certain team members also have participated in a number of other commercial PKI and WebTrust for CA examinations both as a team member and as a quality reviewer. We have incorporated consultations with other EY staff who represent the firm on the AICPA WebTrust Task Force. EY's client roster for PKI projects for governmental agencies other than the GPO includes other US federal agencies as well as foreign governmental monetary organizations.

We are available if you need any additional information or would like to further discuss this memorandum.

Ernst + Young LLP

August 30, 2010

ERNST & YOUNG

Summary information for Ernst & Young executives assigned to the engagement				
Name	**Rank**	**Certifications**	**Years of experience**	**In compliance with EY CPE policy (Yes/No)**
Werner Lippuner	Principal	CA (Switzerland), CISA, CISM	20	Yes
James Merrill	Executive Director	CPA, CISA	26	Yes
Christopher Kostick	Executive Director	CISSP	23	Yes
Timothy Iijima	Senior Manager	PMO	13	Yes

U.S. GOVERNMENT PRINTING OFFICE
KEEPING AMERICA INFORMED

Assertion of Management as to its Disclosure of its Business Practices and its Controls Over its Certification Authority Operations during the period from July 1, 2009 through June 30, 2010

August 30, 2010

The U.S. Government Printing Office (GPO) operates a certification authority (CA) service known as the GPO Public Key Infrastructure Certification Authority (GPO-CA) in Washington, DC and provides the following CA services:

- Subscriber registration
- Certificate rekey
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate status information processing
- Integrated circuit card life cycle management

Management of GPO is responsible for establishing and maintaining effective controls over its CA operations, including CA business practices disclosure in GPO's Certificate Practices Statement, service integrity (including key and certificate life cycle management controls), and CA environmental controls. These controls contain monitoring mechanisms, and actions are taken to correct deficiencies identified.

There are inherent limitations in any controls, including the possibility of human error and the circumvention or overriding of controls. Accordingly, even effective controls can provide only reasonable assurance with respect to GPO-CA's operations. Furthermore because of changes in conditions, the effectiveness of controls may vary over time.

Management of GPO has assessed the controls over its CA operations. Based on that assessment, in GPO management's opinion, in providing its CA services known as GPO-CA in Washington, DC, during the period from July 1, 2009 through June 30, 2010. GPO has:

- Disclosed its key and certificate life cycle management business and information privacy practices in its Certificate Practices Statement, and provided such services in accordance with its disclosed practices;
- Maintained effective controls to provide reasonable assurance that:

- Subscriber information was properly authenticated (for the registration activities performed by GPO);
- The integrity of keys and certificates it managed was established and protected throughout their life cycles;
- Subscriber and relying party information was restricted to authorized individuals and protected from uses not specified in the GPO's CA business practices disclosure;
- The continuity of key and certificate life cycle management operations was maintained, and
- CA systems development, maintenance and operations were properly authorized and performed to maintain CA systems integrity

based on the AICPA/CICA WebTrust for Certification Authorities Criteria, including the following:

CA Business Practices Disclosure

Service Integrity

Key Life Cycle Management Controls

CA Key Generation
CA Key Storage, Backup, and Recovery
CA Public Key Distribution
CA Key Usage
CA Key Destruction
CA Key Archival
CA Cryptographic Hardware Life Cycle Management
CA-Provided Subscriber Key Management Services

Certificate Life Cycle Management Controls

Subscriber Registration
Certificate Rekey
Certificate Issuance
Certificate Distribution
Certificate Revocation
Certificate Status Information Processing
Integrated Circuit Card Life Cycle Management

CA Environmental Controls

Certification Practice Statement and Certificate Policy Management
Security Management
Asset Classification and Management
Personnel Security
Physical and Environmental Security
Operations Management
System Access Management
Systems Development and Maintenance

Business Continuity Management
Monitoring and Compliance
Event Journaling

Michael Wash
Chief Information Officer

John Hannan
Chief Information Security Officer

Appendix: Webtrust Criteria further explanation

The following was provided by GPO as additional information about their assertion:

Maintained effective controls to provide reasonable assurance that:

- Subscriber information was properly authenticated (for the registration activities performed by GPO);
  - Procedures defined in Section 1 (Introduction) of the GPO CPS are in place and operational.
  - Procedures defined in Section 3 (Identification and Authentication) of the GPO CPS are in place and operational.
- The integrity of keys and certificates it managed was established and protected throughout their life cycles;
  - Procedures defined in Section 2 (Publication and Repository Responsibilities) of the GPO CPS are in place and operational.
  - Procedures defined in Section 4 (Certificate Life Cycle) of the GPO CPS are in place and operational.
  - Procedures defined in Section 6 (Technical Security Controls) of the GPO CPS are in place and operational.
  - Procedures defined in Section 7 (Certificate, CARL/CRL and OCSP Profiles Format) of the GPO CPS are in place and operational.
- Subscriber and relying party information was restricted to authorized individuals and protected from uses not specified in the GPO's CA business practices disclosure;
  - Procedures defined in Section 5 (Facility Management and Operations Controls) of the GPO CPS are in place and operational.
  - Procedures defined in Section 8 (Compliance Audit and other Assessments) of the GPO CPS are in place and operational.
  - Procedures defined in Section 9 subsections 9.4.4 (Privacy of Personal Information – Responsibility to Protect Private Information) and 9.6.3 (Representations and Warranties – Subscriber Representations and Warranties) are in place and operational.
- The continuity of key and certificate life cycle management operations was maintained, and
- CA systems development, maintenance and operations were properly authorized and performed to maintain CA systems integrity

Appendix. Report Distribution

Public Printer
Deputy Public Printer
Acting Chief Management Officer
Chief Information Officer
Chief Technology Officer
Chief Information Security Officer