



U.S. GOVERNMENT PRINTING OFFICE  
OFFICE OF INSPECTOR GENERAL

ASSESSMENT REPORT

09-11

---

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

**September 23, 2009**

---

**Date**

September 23, 2009

**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 09-11**

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 2009. 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 PKI is cross-certified with the Federal Bridge Certificate Authority (FBCA). FBCA certification provisions require the GPO PKI to undergo a compliance review. To satisfy this compliance requirement, the OIG tasked E&Y to conduct a WebTrust 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 WebTrust assessment also satisfies Microsoft Root CA distribution<sup>1</sup> compliance audit requirements.

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.
- 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.

This Attestation Report covers the period July 1, 2008 through June 30, 2009. 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.

---

<sup>1</sup> The Microsoft Root CA program was established to better protect Microsoft customers from security issues related to the use of PKI certificates. CA providers are required to complete a WebTrust for Certification Authorities examination or provide an equivalent third-party attestation.

**In the event of 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 us 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.

A handwritten signature in black ink that reads "Kevin J. Carson". The signature is fluid and cursive, with "Kevin" on top and "J. Carson" below it.

Kevin J. C Carson  
Assistant Inspector General for Audits and Inspections

Enclosure

## Enclosure



**ERNST & YOUNG**

Ernst & Young  
8484 Westpark Drive  
McLean, Virginia 22102  
Tel: +1 703 747 1000  
[www.ey.com](http://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, 2008 through June 30, 2009, 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

A member firm of Ernst & Young Global Limited

## Enclosure



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.

In our opinion, for the period from July 1, 2008 through June 30, 2009, 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.

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.

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 14, 2009

**Enclosure**



**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, 2008 through June 30, 2009**

August 14, 2009

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

GPO-CA makes use of external registration authorities for specific subscriber registration activities as disclosed in GPO's business practice disclosures.

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.

The GPO CPS conforms to the requirements of the GPO CP.

The GPO-CA is operated in conformance with the requirements of the GPO CPS.

The GPO-CA is operated in conformance with the requirements of all current cross-certification Memorandum of Agreements (MOAs) executed by the GPO-CA.

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, 2008 through June 30, 2009, 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:
  - Procedures defined in Section 1 (Introduction) of the GPO CPS are in place and operational.

## Enclosure

- Maintained effective controls to provide reasonable assurance that:
  - Subscriber information was properly authenticated (for the registration activities performed by GPO);
    - o 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;
    - o Procedures defined in Section 2 (Publication and Repository Responsibilities) of the GPO CPS are in place and operational.
    - o Procedures defined in Section 4 (Certificate Life Cycle) of the GPO CPS are in place and operational.
    - o Procedures defined in Section 6 (Technical Security Controls) of the GPO CPS are in place and operational.
    - o 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;
    - o Procedures defined in Section 5 (Facility Management and Operations Controls) of the GPO CPS are in place and operational.
    - o Procedures defined in Section 8 (Compliance Audit and other Assessments) of the GPO CPS are in place and operational.
    - o 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

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

**Enclosure**

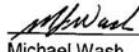
CA Key Archival  
CA Cryptographic Hardware Life Cycle Management  
CA-Provided Subscriber Key Management Services

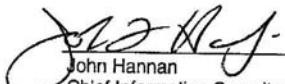
**Certificate Life Cycle Management Controls**

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

## Enclosure



**ERNST & YOUNG**

Ernst & Young  
8484 Westpark Drive  
McLean, Virginia 22102

Tel: +1 703 747 1000  
[www.ey.com](http://www.ey.com)

August 14, 2009

### **Letter of supplementary information**

To the Inspector General of the United States Government Printing Office (GPO or the Agency), and the Management of GPO 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's compliance with specified requirements.

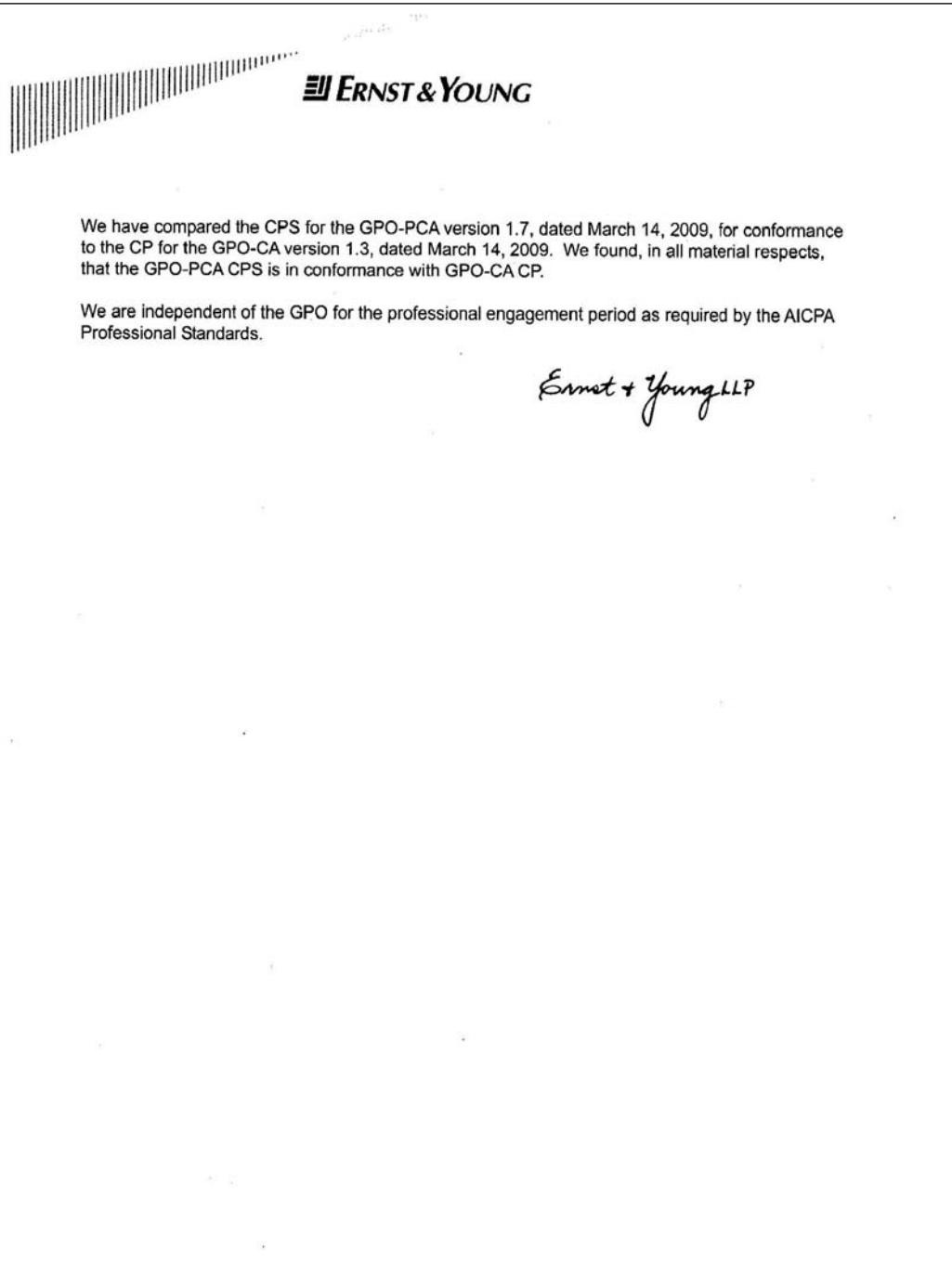
The audit period for this examination was from July 1, 2008 through June 30, 2009. Our examination was performed between May 26, 2009 and August 14, 2009.

We examined the Certificate Policy (CP) for the GPO-CA version 1.3, dated March 14, 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.

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, 2009, we reported that management's assertion was fairly stated in all material respects.

A member firm of Ernst & Young Global Limited

**Enclosure**



## **APPENDIX. REPORT DISTRIBUTION**

---

Deputy Public Printer  
Chief of Staff  
Acting General Counsel  
Chief Management Officer  
Chief Information Officer  
Chief Technology Officer  
Chief Information Security Officer