



**U.S. GOVERNMENT PUBLISHING OFFICE**  
**OFFICE OF INSPECTOR GENERAL**

**ASSESSMENT REPORT**  
**REPORT NUMBER 15-21**

---

**Webtrust for Certification Authority**  
**September 24, 2015**

---



**U.S. GOVERNMENT PUBLISHING OFFICE**  
**OFFICE OF INSPECTOR GENERAL**

**Date**

September 24, 2015

**To**

Chief Information Officer

**From**

Inspector General

**Subject**

Assessment Report - Webtrust for Certification Authority  
Report Number 15-21

Enclosed please find the subject final report. The Office of the Inspector General contracted with Ernst & Young LLP (E&Y) to provide an opinion on the Government Publishing Office's (GPO) assertions regarding their certification authority process for July 1, 2014 through June 30, 2015. E&Y conducted their work in accordance with attestation standards established by the American Institute of Certified Public Accountants.

E&Y concluded that GPO's assertion is fairly stated in all material respects. E&Y is responsible for the attached report and the opinion expressed therein.

We appreciate the courtesies extended to E&Y and to our audit staff. If you have any questions or comments about this report, please do not hesitate to contact Mr. Phillip M. Faller, Assistant Inspector General for Audits and Inspections at (202) 512-2009 or me at (202) 512-0039.

A handwritten signature in cursive script that reads "Michael A. Raponi".

MICHAEL A. RAPONI  
Inspector General

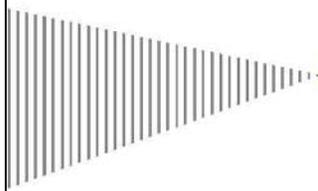
**Attachment**

cc:

Director, GPO  
Deputy Director, GPO  
General Counsel  
Chief of Staff  
Chief Administrative Office

# U.S. Government Printing Office

Report of Independent Accountants  
WebTrust for CA  
For the Period July 1, 2014 to June 30, 2015



**Table of Contents**

Report of Independent Accountants..... 1  
Management Assertion ..... 3

## 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:

We have examined the [assertion](#) by the management of the U.S. Government Printing Office Certification Authority (GPO-CA), that in providing its Certification Authority (CA) services in Washington, D.C. for the Principal CA (GPO-PCA) and the Subordinate CA (GPO-SCA) during the period July 1, 2014 through June 30, 2015, it

- ▶ Disclosed its Business, Key Life Cycle Management, Certificate Life Cycle Management, and CA Environmental Control practices in its [Principal Certification Practice Statement](#), [Subordinate Certification Practice Statement](#) and [Certificate Policy](#).
- ▶ Maintained effective controls to provide reasonable assurance that:
  - ▶ GPO-CA's Principal Certification Practice Statement is consistent with its Certificate Policy
  - ▶ GPO-CA's Subordinate Certification Practice Statement is consistent with its Certificate Policy
  - ▶ GPO-CA provided its services in accordance with its Certificate Policy, Principal Certification Practice Statement and Subordinate Certification Practice Statement
- ▶ Maintained effective controls to provide reasonable assurance that:
  - ▶ The integrity of keys and certificates it managed was established and protected throughout their life cycles;
  - ▶ The integrity of subscriber keys and certificates it managed was established and protected throughout their life cycles;
  - ▶ The Subscriber information was properly authenticated; and
  - ▶ Subordinate CA certificate requests were accurate, authenticated and approved.
- ▶ Maintained effective controls to provide reasonable assurance that:
  - ▶ Logical and physical access to CA systems and data was restricted to authorized individuals;
  - ▶ The continuity of key and certificate management operations was maintained; and

- ▶ CA systems development, maintenance and operations were properly authorized and performed to maintain CA systems integrity

based on the [Trust Services Principles and Criteria for Certification Authorities, Version 2.0](#).

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

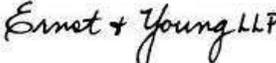
Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants, and accordingly, included (1) obtaining an understanding of GPO-CA's key and certificate life cycle management business practices and its controls over key and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

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.

Because of the nature and inherent limitations of controls, GPO-CA's ability to meet the aforementioned criteria may be affected. For example, controls may not prevent, or detect and correct error, fraud, unauthorized access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

In our opinion, for the period July 1, 2014 through June 30, 2015, GPO-CA's management's assertion, as set forth in the first paragraph, is fairly stated, in all material respects, based on the [Trust Services Principles and Criteria for Certification Authorities Criteria, Version 2.0](#).

This report does not include any representation as to the quality of GPO-CA's services beyond those covered by the [Trust Services Principles and Criteria for Certification Authorities Version 2.0](#) criteria, nor the suitability of any of GPO-CA's services for any customer's intended purpose.

Ernst & Young LLP

September 21, 2015



**Assertion by Management Regarding Its  
Disclosure of Its Business Practices and Its Controls Over its  
Certification Authority Operations During the  
Period July 1, 2014 Through June 30, 2015**

September 21, 2015

The U.S. Government Printing Office (GPO) operates Certification Authority (CA) services known as GPO-CA. GPO-CA, as a Root CA, provides the following certification authority 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. Management of GPO has assessed the disclosure of its certificate practices and its controls over its CA services. Based on that assessment, in GPO Management's opinion, in providing its CA services in Washington D.C. for the Principal CA: GPO-PCA and the Subordinate CA: GPO-SCA, during the period July 1, 2014 through June 30, 2015, GPO has:

- Disclosed its Business, Key Life Cycle Management, Certificate Life Cycle Management, and CA Environmental Control practices in its Principal Certification Practice Statement, Subordinate Certification Practice Statement and Certificate Policy.
- Maintained effective controls to provide reasonable assurance that:
  - GPO-CA's Certification Practice Statements were consistent with its Certificate Policy
  - GPO-CA provided its services in accordance with its Certificate Policy and Certification Practice Statements
- Maintained effective controls to provide reasonable assurance that:
  - The integrity of keys and certificates it managed was established and protected throughout their life cycles;
  - The integrity of subscriber keys and certificates it managed was established and protected throughout their life cycles;



- The Subscriber information was properly authenticated; and
- Subordinate CA certificate requests were accurate, authenticated and approved.
- Maintained effective controls to provide reasonable assurance that:
  - Logical and physical access to CA systems and data was restricted to authorized individuals;
  - The continuity of key and certificate management operations was maintained; and
  - CA systems development, maintenance and operations were properly authorized and performed to maintain CA systems integrity

for the Principal CA: GPO-PCA and the Subordinate CA: GPO-SCA, based on the Trust Services Principles and Criteria for Certification Authorities, Version 2.0 including the following:

**CA Business Practices Disclosure**

CA Business Practices Management  
Certificate Policy Management  
Certification Practice Statement Management  
CP and CPS Consistency

**Service Integrity**

CA Key Life Cycle Management Controls  
CA Key Generation  
CA Key Storage, Backup, and Recovery  
CA Public Key Distribution  
CA Key Usage  
CA Key Compromise  
CA Cryptographic Hardware Life Cycle Management

Subscriber Key Life Cycle Management Controls  
CA- Provided Subscriber Key Generation Services  
CA-Provided Subscriber Key Storage and Recovery Services  
Integrated Circuit Card (ICC) Life Cycle Management  
Requirements for Subscriber Key Management

Certificate Life Cycle Management Controls  
Subscriber Registration  
Certificate Rekey  
Certificate Issuance  
Certificate Distribution



Certificate Revocation  
Certificate Validation  
Subordinate CA Certificate Life Cycle Management Controls  
Subordinate CA Certificate Life Cycle Management

**CA Environmental Controls**

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  
Audit Logging

Very truly yours,

  
Charles Riddle  
GPO Chief Information Officer

EY | Assurance | Tax | Transactions | Advisory

**About EY**

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization and may refer to one or more of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit [ey.com](http://ey.com).

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

© 2015 Ernst & Young LLP.  
All Rights Reserved.

BSC No. 1509-1668885  
ED none