U.S. GOVERNMENT PUBLISHING OFFICE
OFFICE OF INSPECTOR GENERAL

ASSESSMENT REPORT
REPORT NUMBER 19-12

Federal PKI Compliance Report
September 16, 2019

U.S. GOVERNMENT PUBLISHING OFFICE
OFFICE OF INSPECTOR GENERAL

Date

September 16, 2019

To

Acting Deputy Director

From

Inspector General

Subject:

Assessment Report — Federal PKI Compliance
Report Number 19-12

Enclosed please find the subject final report. The Office of Inspector General (OIG) contracted with Ernst & Young LLP (E&Y) to provide a compliance report of the Government Publishing Office's (GPO) Public Key Infrastructure (PKI) for July 1, 2018 through June 30, 2019. E&Y conducted its 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 also concluded that the GPO Principal Certification Authority Certificate Practices Statement conformed in all material respects to the GPO-Certificate Authority and Federal PKI common policies. 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. Freddie W. Hall, Assistant Inspector General for Audits and Inspections at (202) 512-1597 or me at (202) 512-0039.

MICHAEL P. LEARY
Inspector General

Attachment
cc:
Acting General Counsel, GPO
Acting Chief of Staff, GPO
Chief Information Officer, GPO

Contents

U.S. Government Printing Office

Report of Independent Accountants
Federal PKI Compliance Report

For the Period July 1, 2018 to June 30, 2019

EY
Building a better working world

Table of Contents

Ernst & Young LLP
1775 Tysons Blvd
Tysons, VA 22102

Tel: +1 703 747 1000
Fax: +1 703 747 0100
ey.com

Report of Independent Accountants

To the Inspector General of the United States Government Printing Office,
the Management of the United States Government Printing Office Certification Authority, and
the Federal PKI Policy Authority:

We have examined management's assertion about the United States Government Printing Office Certification Authority's (GPO-CA) compliance with requirements of its Certificate Policy Version 1.8 dated April 5, 2019 (GPO-CA CP); its Principal Certificate Practices Statement Version 1.8 dated April 5, 2019 (GPO-PCA CPS); its Subordinate Certificate Practices Statement Version 1.8 dated April 5, 2019 (GPO-SCA CPS); and its Memorandum of Agreement dated August 1, 2017 between the Federal PKI Policy Authority and GPO-CA (GPO-MOA) for the period July 1, 2018 through June 30, 2019. Management is responsible for the assertion. Our responsibility is to express an opinion on management's assertion about GPO-CA's compliance based on our examination.

Our examination was conducted in accordance with the attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risks of material misstatement of management's assertion, whether due to fraud or error. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination was not conducted for the purpose of evaluating management's cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on management's cybersecurity risk management program.

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.

Our examination was limited to (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 the 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

Building a better working world

as we considered necessary in the circumstances. Because of their nature and inherent limitations, controls may not prevent, or detect and correct, all errors or fraud that may be considered relevant. Furthermore, the projection of any evaluations of effectiveness to future periods is subject to the risk that controls may become inadequate because of changes in conditions, that the degree of compliance with such controls may deteriorate, or that changes made to the system or controls, or the failure to make needed changes to the system or controls, may alter the validity of such evaluations.

The GPO-CA operates a Principal Root CA (GPO-PCA) and it's Subordinate CA (GPO-SCA). Multiple Root CAs were not in operation at GPO-CA. We examined the GPO-PCA CPS for conformance to the GPO-CA CP. We have also compared the GPO-SCA CPS for conformance to the GPO-CA CP. We found, in all material respects, that the GPO-PCA CPS and the GPO-SCA CPS are in conformance with GPO-CA CP.

We examined the GPO-PCA CPS and the GPO-SCA CPS for conformance to the Federal Bridge Certification Authority (FBCA) Certificate Policy Version 2.35 dated April 15, 2019 (FBCA-CP). We found, in all material respects, that the GPO-PCA CPS and the GPO-SCA CPS are in conformance with the requirements of the FBCA-CP.

We evaluated GPO-CA's operations, including activity performed by Registrant Authorities (RAs) on behalf of GPO-CA, for conformance to the requirements of the GPO-PCA CPS and the GPO-SCA CPS and we evaluated GPO-CA's operations for conformance to the requirements of the current cross-certification Memorandum of Agreement dated August 1, 2017 between the Federal PKI Policy Authority and the GPO-CA (GPO-MOA).

In our opinion, GPO-CA management's assertion referred to above is fairly stated, in all material respects for the period July 1, 2018 through June 30, 2019.

The examination was conducted by Ernst & Young professionals. The qualifications of the professionals are further described in Exhibit I - Summary of matters related to project personnel. Our fieldwork examination procedures were primarily performed between April 1, 2019 and August 15, 2019.

We are independent with respect to the United States Government Printing Office within Rule 1.200 of the Code of Professional Conduct of the American Institute of Certified Public Accountants.

This report does not include any representation as to the quality of GPO-CA's services beyond those covered by the Chartered Professional Accountants of Canada ("CPA Canada") *WebTrust Services Criteria for Certification Authorities Version 2.1*, nor the suitability of any of GPO-CA's services for any customer's intended purpose.

This report is intended solely for the information and use of GPO-CA and the Federal PKI Policy Authority and is not intended to be, and should not be, used by anyone other than GPO-CA and the Federal PKI Policy Authority.

Ernst & Young LLP

September 12, 2019

Exhibit 1 – Summary of matters related to project personnel

As part of the WebTrust for Certification Authority (WTCA) examination services provided to GPO-CA, in accordance with relevant American Institute of Certified Public Accountants (AICPA) standards, 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 examination. 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 service line. Recruiting for the Advisory practice focuses on candidates with information technology, accounting, finance and other business-related degrees.

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.

Methodologies, policies and procedures

EY Professionals carrying out WTCA examinations are required to comply with EY's policies for performing examinations in accordance with the attestation standards established by the American Institute of Certified Public Accountants.

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 Advisory are required to obtain a professional certification to be promoted to Manager. In the Advisory 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.

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. 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.
- 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, CISA) may be subject to continuing education requirements as part of that designation or certification.

Experience Auditing PKI Systems

The EY executive team assigned to the GPO project has experience in performing audits and/or examinations 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 personnel who represent the firm on the WebTrust for CA Task Force.

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

Summary information for EY executives assigned to the engagement				
Name	**Rank**	**Certifications**	**Years of experience**	**In compliance with EY CPE policy (Yes/No)**
Mike Herrinton	Partner	CPA	32	Yes
James Merrill	Managing Director	CPA, CISA	36	Yes
Donoghue Clarke	Principal	CISSP, CIPP, CISA	14	Yes
Clayton Brothers	Senior	CISSP, CISA	5	Yes

Assertion of Management on its
Business Practices Disclosures and Controls over its
Certificate Authority Operations during the
Period of July 1, 2018 through June 30, 2019

September 12, 2019

The U.S. Government Printing Office (GPO) operates Certification Authority (CA) services at Washington D.C. for the Principal CA (GPO-PCA) and the Subordinate CA (GPO-SCA).

GPO's CA services provide the following certification authority services:

- Subscriber registration
- Certificate rekey
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Subscriber key generation and management

Management of GPO is responsible for establishing and maintaining effective controls over its CA operations. With respect to our compliance with requirements in the GPO Certificate Policy Version 1.8 dated April 5, 2019 (GPO-CA CP); its Principal Certificate Practices Statement Version 1.8 dated April 5, 2019 (GPO-PCA CPS); its Subordinate Certificate Practices Statement Version 1.8 dated April 5, 2019 (GPO-SCA CPS); and its Memorandum of Agreement dated August 1, 2017 between the Federal PKI Policy Authority and GPO-CA (GPO-MOA) for the period July 1, 2018 through June 30, 2019, GPO has:

Disclosed its Business, Key Life Cycle Management, and Certificate Life Cycle Management, and CA Environmental Control practices as below:

- GPO CP v 1.8
- GPO-PCA CPS v 1.8
- GPO-SCA CPS v 1.8

Maintained effective controls to provide reasonable assurance that:

- GPO-CA's Certification Practice Statements are consistent with its Certificate Policy
- GPO-CA provides 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 manages was established and protected throughout their life cycles;
  - Procedures defined in Section 2 (Publication and Repository Responsibilities) of the GPO-PCA CPS and GPO-SCA CPS were in place and operational.

- Procedures defined in Section 4 (Certificate Life Cycle) of the GPO-PCA CPS and the GPO-SCA CPS were in place and operational.
- Procedures defined in Section 6 (Technical Security Controls) of the GPO-PCA CPS and the GPO-SCA CPS were in place and operational.
- Procedures defined in Section 7 (Certificate, CRL and OCSP Profiles) of the GPO-PCA CPS and the GPO-SCA CPS were in place and operational.

- The integrity of subscriber keys and certificates it manages was established and protected throughout their life cycles;
  - Procedures defined in Section 4 (Certificate Life Cycle) of the GPO-PCA CPS and the GPO-SCA CPS were in place and operational.
  - Procedures defined in Section 6 (Technical Security Controls) of the GPO-PCA CPS and the GPO-SCA CPS were in place and operational.

- The Subscriber information was properly authenticated; and
  - Procedures defined in Section 1 (Introduction) of the GPO-PCA CPS and GPO-SCA CPS were in place and operational.
  - Procedures defined in Section 3 (Identification and Authentication) of the GPO-PCA CPS and GPO-SCA CPS were in place and operational.

- Subordinate CA certificate requests were accurate, authenticated and approved
  - Procedures defined in Section 4 (Certificate Life Cycle) of the GPO-PCA CPS and the GPO-SCA CPS were in place and operational.

Maintained effective controls to provide reasonable assurance that:

- Logical and physical access to CA systems and data was restricted to authorized individuals;
  - Procedures defined in Section 5 (Facility Management and Operational Controls) of the GPO-PCA CPS and the GPO-SCA CPS were in place and operational.
  - Procedures defined in Section 8 (Compliance Audit and other Assessments) of the GPO-PCA CPS and the GPO-SCA CPS were 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 Representatives and Warranties) of the GPO-PCA CPS and the GPO-SCA CPS were in place and operational.

- The continuity of key and certificate management operations was maintained; and
  - Procedures defined in Section 5 (Facility Management and Operational Controls) of the GPO-PCA CPS and the GPO-SCA CPS were in place and operational.

- GPO-CA's Certification Practice Statements are consistent with its Certificate Policy
- GPO-CA provides 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 manages was established and protected throughout their life cycles;
The integrity of subscriber keys and certificates it manages 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 Root Keys listed in Appendix A, based on the Chartered Professional Accountants of Canada ("CPA Canada") *WebTrust Services Principles and Criteria for Certification Authorities 2.1.*, including the following:

CA Business Practices Disclosure
- Certification Practice Statement (CPS)
- Certificate Policy (CP)

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

CA Environmental Controls
- Security Management
- Asset Classification and Management
- Personnel Security
- Physical & Environmental Security
- Operations Management
- System Access Management
- System Development and Maintenance
- Business Continuity Management
- Monitoring and Compliance
- Audit Logging

CA Key Lifecycle Management Controls
- CA Key Generation
- CA Key Storage, Backup, and Recovery
- CA Public Key Distribution

8

- CA Key Usage
- CA Key Archival and Destruction
- CA Key Compromise
- CA Cryptographic Hardware Lifecycle Management
- CA Key Escrow

Subscriber Key Lifecycle Management Controls

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

Certificate Lifecycle Management Controls

- Subscriber Registration
- Certificate Renewal
- Certificate Rekey
- Certificate Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Suspension
- Certificate Validation

Subordinate CA Certificate Lifecycle Management Controls

- Subordinate CA Certificate Lifecycle Management

Very truly yours,

Sam S. Musa
Chief Information Officer

John Hannan
Chief Information Security Officer

Appendix A

Root/Subordinate Name	Subject Key Identifier	Certificate Serial Number	SHA-1 Fingerprint
OU = GPO PCA OU = Certification Authorities OU = Government Printing Office O = U.S. Government C = US	KeyID=22 71 78 21 b5 84 6d b3 01 e3 12 74 41 4e 4d 45 07 e9 52 ff	40 d8 6a 17	cc b9 4f 7c 2e ce a4 85 30 64 9c 00 17 50 35 65 24 ca b0 5f
OU = GPO SCA OU = Certification Authorities OU = Government Printing Office O = U.S. Government C = US	KeyID=21 a2 8c 76 a2 0d c6 bb 4e 08 45 ec 5f c4 82 27 9a 89 93 25	40 d8 6a 4f	b9 14 fd a0 c3 a0 ee 78 f8 fa 28 4d 3c 82 28 8c e2 f6 0e a5

Appendix A-1 – Report Distribution

Acting General Counsel, GPO
Acting Chief of Staff, GPO
Chief Information Officer, GPO

Major Contributor to the Report

Tony Temsupasiri – Lead Information Technology Specialist