KPMG LLP
Mission Towers I
Suite 100
3975 Freedom Circle Drive
Santa Clara, CA 95054

Independent Accountant's Report

To the Management of
Aetna Life Insurance Company:

We have examined the assertion by the management of Aetna Life Insurance Company ("Aetna"), for its Certification Authority (CA) operations in Hartford, Middletown, and Windsor, Connecticut, regarding the disclosure of its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its Certification Practice Statement, the provision of services in accordance with its Certification Practice Statement, and the effectiveness of 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 lifecycle management operations, and over development, maintenance, and operation of CA systems integrity throughout the period from January 1, 2015 to December 31, 2015 for the Aetna Inc. Certificate Authority (the "Aetna CA").

The management of Aetna is responsible for its assertion. Our responsibility is to express an opinion based on our examination.

We conducted our examination in accordance with standards for attestation engagements established by the American Institute of Certified Public Accountants and, accordingly, included:

(1) obtaining an understanding of Aetna's key and certificate lifecycle 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 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 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.

During our examination, we noted the following issues that resulted in a modification of our opinion:

#	WebTrust for CAs Criteria Requirements	Issues Noted
1	WebTrust for Certification Authorities (WebTrust for CAs) Criterion 2.2 requires that: The CA maintains controls to provide reasonable assurance that its Certification Practice Statement (CPS) management processes are effective.	It was noted that the CPS had not been updated or reviewed since 2011 and there is no process in place to update the CPS periodically. We also noted that Aetna's CA operations were inconsistent with the practices specified in the CPS including; Identification, Application Requirements, Certificate Information, Certificate Revocation, Physical Access Controls, CA Key Pair, Business Continuity Management, and Event Logging. This caused WebTrust for CAs Criterion 2.2 not to be met.

#	WebTrust for CAs Criteria Requirements	Issues Noted
2	WebTrust for CAs Criterion 3.1 requires that: The CA maintains controls to provide reasonable assurance that: • Security risks are identified and managed.	It was noted that a security risk assessment of the Aetna CA operations was not performed during the examination period. This caused WebTrust for CAs Criterion 3.1 not to be met.
3	WebTrust for CAs Criterion 3.2 requires that: The CA maintains controls to provide reasonable assurance that CA assets and subscriber and relying party information receive an appropriate level of protection based upon identified risks and in accordance with the CA's disclosed business practices. WebTrust for CAs Criterion 3.4 requires that: The CA maintains controls to provide reasonable assurance that physical access to CA facilities and equipment is limited to authorized individuals, protected through restricted security perimeters, and is operated under multiple person (at least dual custody) control…	It was noted that HSMs are located in the Aetna data center and the CA system is located within the caged area of the data center with single person access enforced. Aetna's CPS Section 4.2 states that, "Access to the Aetna CA facility requires the two authentication factors incorporating biometrics, keys, and proximity cards. Access to the facility requires a minimum of two authorized Aetna employees and is checked at three independent physical locations." However, multiple person control over the areas housing the CA system and HSMs is not enforced, and biometrics are not used. This caused WebTrust for CAs Criteria 3.2 and 3.4 not to be met with respect to the CA system and HSMs.
4	WebTrust for CAs Criterion 3.7 requires that: The CA maintains controls to provide reasonable assurance that CA systems development and maintenance activities are documented, tested, authorized, and properly implemented to maintain CA system integrity.	It was noted that approval was documented for each change but testing was not documented as required for the population of 6 PKI changes made during the examination period. This caused WebTrust for CAs Criterion 3.7 not to be met.
5	WebTrust for CAs Criterion 3.8 requires that: The CA maintains controls to provide reasonable assurance of continuity of operations in the event of a disaster. Such controls include, at a minimum: • the development and testing of a CA business continuity plan that includes a disaster recovery process for critical components of the CA system; • the storage of required cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location; • the storage of backups of systems, data and configuration information at an alternate location; and • the availability of an alternate site, equipment and connectivity to enable recovery.	It was noted that the storage of required cryptographic materials at an alternate location was not in place or defined in the business continuity plan. Further, it was noted that there were no disaster recovery tests performed during the examination period. This caused WebTrust for CAs Criterion 3.8 not to be met.

#	WebTrust for CAs Criteria Requirements	Issues Noted
6	WebTrust for CAs Criterion 3.9 requires that: • The CA maintains controls to provide reasonable assurance that unauthorized CA system usage is detected.	It was noted that the Aetna PKI issuing systems are not reviewed for configuration changes that violate their security policies. Additionally, it was noted that there were no tools implemented to monitor, detect, and report security-related configurations changes to Aetna's Certificate Systems. This caused WebTrust for CAs Criterion 3.9 not to be met.
7	WebTrust for CAs Criterion 3.10 requires that: The CA maintains controls to provide reasonable assurance that: • significant CA environmental, key management, and certificate management events are accurately and appropriately logged; • the confidentiality and integrity of current and archived audit logs are maintained; • audit logs are completely and confidentially archived in accordance with disclosed business practices; and • audit logs are reviewed periodically by authorized personnel.	It was noted that: • physical access to the cage housing the CA system was not logged; • event logs for the CA prior to July 2015 were not available; and • logs are not reviewed periodically. This caused WebTrust for CAs Criterion 3.10 not to be met.
8	WebTrust for CAs Criterion 6.1 requires that: The CA maintains controls to provide reasonable assurance that for authenticated certificates: • Subscribers are accurately identified in accordance with the CA's disclosed business practices; and • Subscriber's certificate requests are accurate, authorized and complete.	The Aetna CPS Section 3.1 states that, "all enrollment forms are subject to review, approval, and acceptance." Aetna compares certificate requests against a pre-validated list of domains and certificate requesters against a list of authorized requesters. However, it was noted that there was no process in place to revalidate the lists of domains and authorized requesters. It was also noted that there were 36 certificates issued to Coventry Health Care, a subsidiary of Aetna, during the examination period and each certificate included incorrect location information. This caused WebTrust for CAs Criterion 6.1 not to be met.

In our opinion, except for the matters described in the preceding table, in providing its Aetna CA services in Hartford, Middletown, and Windsor, Connecticut during the period January 1, 2015 through December 31, 2015, Aetna:

- Disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its Aetna GeoRoot Certification Practice Statement, Version 1.1, dated September 24, 2011 ("Aetna CPS") on the Aetna website

- Maintained effective controls to provide reasonable assurance that:
    - Aetna provides its services in accordance with Aetna's Certification Practice Statement

- 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

- Maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and certificates it manages was established and protected throughout their life cycles; and
  - Subscriber information was properly authenticated (for the registration activities performed by Aetna)

based on the AICPA/CPA Canada WebTrust Principles and Criteria for Certification Authorities v2.0.

The relative effectiveness and significance of specific controls at Aetna 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, Aetna'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.

This report does not include any representation as to the quality of Aetna's services beyond those covered by the AICPA/CPA Canada WebTrust Principles and Criteria for Certification Authorities v2.0, nor the suitability of any of Aetna's services for any customer's intended purpose.

KPMG LLP

Certified Public Accountants
Santa Clara, California
May 11, 2016

Assertion by Management as to
Its Disclosure of Its Business Practices and Its Controls
Over Its Certification Authority Operations
during the period from January 1, 2015 through December 31, 2015

May 11, 2016

Aetna Life Insurance Company ("Aetna") provides the following certification services through its Aetna Inc. Certificate Authority (CA):

- Subscriber registration
- Certificate rekey
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate status information processing

Management of Aetna is responsible for establishing and maintaining effective controls over its CA operations, including CA business practices disclosure in its Aetna GeoRoot Certification Practice Statement, Version 1.1, dated September 24, 2011, 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.

Controls have inherent limitations, 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 Aetna's CA operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

Management has assessed the controls over its Aetna CA operations. Based on that assessment, in Management's opinion, in providing its CA services at Hartford, Middletown, and Windsor, Connecticut, during the period from January 1, 2015 through December 31, 2015, Aetna has –

- Disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its Certification Practice Statement
- 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.
- Maintained effective controls to provide reasonable assurance that:
    - the integrity of keys and certificates it manages was established and protected throughout their life cycles;
    - Subscriber information was properly authenticated (for the registration activities performed by Aetna)

based on the AICPA/CPA Canada WebTrust Principles and Criteria for Certification Authorities including the following:

CA Business Practices Disclosure

- Certification Practice Statement

CA Business Practices Management

- Certification Practice Statement 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

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 Archival and Destruction
- CA Key Compromise
- CA Cryptographic Hardware Life Cycle Management

Subscriber Key Life Cycle Management Controls

- Requirements for Subscriber Key Management

Certificate Life Cycle Management Controls

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

except for the effects of the matters noted below:

#	WebTrust for CAs Criteria Requirements	Issues Noted
1	WebTrust for CAs Criterion 2.2 requires that: The CA maintains controls to provide reasonable assurance that its Certification Practice Statement (CPS) management processes are effective.	It was noted that the CPS had not been updated or reviewed since 2011 and there is no process in place to update the CPS periodically. We also noted that Aetna's CA operations were inconsistent with the practices specified in the CPS including; Identification, Application Requirements, Certificate Information, Certificate Revocation, Physical Access Controls, CA Key Pair, Business Continuity Management, and Event Logging. This caused WebTrust for CAs Criterion 2.2 not to be met.
2	WebTrust for CAs Criterion 3.1 requires that: The CA maintains controls to provide reasonable assurance that: • Security risks are identified and managed.	It was noted that a security risk assessment of the Aetna CA operations was not performed during the examination period. This caused WebTrust for CAs Criterion 3.1 not to be met.
3	WebTrust for CAs Criterion 3.2 requires that: The CA maintains controls to provide reasonable assurance that CA assets and subscriber and relying party information receive an appropriate level of protection based upon identified risks and in accordance with the CA's disclosed business practices. WebTrust for CAs Criterion 3.4 requires that: The CA maintains controls to provide reasonable assurance that physical access to CA facilities and equipment is limited to authorized individuals, protected through restricted security perimeters, and is operated under multiple person (at least dual custody) control…	It was noted that HSMs are located in the Aetna data center and the CA system is located within the caged area of the data center with single person access enforced. Aetna's CPS Section 4.2 states that, "Access to the Aetna CA facility requires the two authentication factors incorporating biometrics, keys, and proximity cards. Access to the facility requires a minimum of two authorized Aetna employees and is checked at three independent physical locations." However, multiple person control over the areas housing the CA system and HSMs is not enforced, and biometrics are not used. This caused WebTrust for CAs Criteria 3.2 and 3.4 not to be met with respect to the CA system and HSMs.
4	WebTrust for CAs Criterion 3.7 requires that: The CA maintains controls to provide reasonable assurance that CA systems development and maintenance activities are documented, tested, authorized, and properly implemented to maintain CA system integrity.	It was noted that approval was documented for each change but testing was not documented as required for the population of 6 PKI changes made during the examination period. This caused WebTrust for CAs Criterion 3.7 not to be met.

#	WebTrust for CAs Criteria Requirements	Issues Noted
5	WebTrust for CAs Criterion 3.8 requires that: The CA maintains controls to provide reasonable assurance of continuity of operations in the event of a disaster. Such controls include, at a minimum: • the development and testing of a CA business continuity plan that includes a disaster recovery process for critical components of the CA system; • the storage of required cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location; • the storage of backups of systems, data and configuration information at an alternate location; and • the availability of an alternate site, equipment and connectivity to enable recovery.	It was noted that the storage of required cryptographic materials at an alternate location was not in place or defined in the business continuity plan. Further, it was noted that there were no disaster recovery tests performed during the examination period. This caused WebTrust for CAs Criterion 3.8 not to be met.
6	WebTrust for CAs Criterion 3.9 requires that: • The CA maintains controls to provide reasonable assurance that unauthorized CA system usage is detected.	It was noted that the Aetna PKI issuing systems are not reviewed for configuration changes that violate their security policies. Additionally, it was noted that there were no tools implemented to monitor, detect, and report security-related configurations changes to Aetna's Certificate Systems. This caused WebTrust for CAs Criterion 3.9 not to be met.
7	WebTrust for CAs Criterion 3.10 requires that: The CA maintains controls to provide reasonable assurance that: • significant CA environmental, key management, and certificate management events are accurately and appropriately logged; • the confidentiality and integrity of current and archived audit logs are maintained; • audit logs are completely and confidentially archived in accordance with disclosed business practices; and • audit logs are reviewed periodically by authorized personnel.	It was noted that: • physical access to the cage housing the CA system was not logged; • event logs for the CA prior to July 2015 were not available; and • logs are not reviewed periodically. This caused WebTrust for CAs Criterion 3.10 not to be met.

#	WebTrust for CAs Criteria Requirements	Issues Noted
8	WebTrust for CAs Criterion 6.1 requires that: The CA maintains controls to provide reasonable assurance that for authenticated certificates: • Subscribers are accurately identified in accordance with the CA's disclosed business practices; and • Subscriber's certificate requests are accurate, authorized and complete.	The Aetna CPS Section 3.1 states that, "all enrollment forms are subject to review, approval, and acceptance." Aetna compares certificate requests against a pre-validated list of domains and certificate requesters against a list of authorized requesters. However, it was noted that there was no process in place to revalidate the lists of domains and authorized requesters. It was also noted that there were 36 certificates issued to Coventry Health Care, a subsidiary of Aetna, during the examination period and each certificate included incorrect location information. This caused WebTrust for CAs Criterion 6.1 not to be met.

Aetna Life Insurance Company

Brian Heemsoth
Director, Information Security