Aetna Life Insurance Company

Aetna PKI Infrastructure

Aetna GeoRoot Certificate Practice Statement

Revision and Signoff Sheet

Change Record

Date	Author	Version	Change reference
05/31/2005	JN	.1	Initial draft for review/discussion
06/06/2005	TT	1.0	First candidate for approval
09/20/2011	BH/DP	1.1	Updated to reflect current policies & procedures

Reviewers

Initials	Version approved	Department	Date
TT	1.0	Information Security	06/06/2005
TT	1.1	Information Security	09/24/2011

Table of Contents

1 INTRODUCTION

1.1 Overview

This Aetna Certificate Practice Statement (the "CPS") presents the principles and procedures Aetna employs in the issuance and life cycle management of the Aetna GeoRoot Certification Authority (CA) for the issuance and management of web server SSL certificates. GeoRoot allows Aetna, Inc. to maintain control over certificate lifecycle management, including issuance, renewal and revocation. Functions such as authenticating individuals, deploying and managing SSL certificates and client certificates, and managing the distribution of public keys to appropriate parties all lie internally.

GeoRoot works seamlessly with Microsoft Active Directory and Microsoft Certificate Services for the authentication and delivery of GeoTrust-signed certificates.

This CPS and any and all amendments thereto are incorporated by reference into all of the above-listed Aetna SSL Certificates.

1.1.1 Identification

This CPS complies with GeoTrust's Certificate Policy.

This CPS is titled Aetna GeoRoot Certificate Practice Statement

1.1.2 Community and applicability

The Aetna GeoRoot CA will sign and issue end user SSL (web servers or application servers) certificates within the organization.

1.1.3 Certificate Authorities (CAs)

The Aetna GeoRoot CA, operating under the Microsoft Certificate Services will sign certificates that bind subscribers (e.g., end users, web servers, application servers, subordinate CAs) to their private keys.

The Aetna GeoRoot CA, operating under Microsoft Certificate Services, are responsible for:

- **Signature**
  - The creation and signing of certificates binding CAs, subscribers, end users and as required subordinate CAs with their signature verification keys;
  - Promulgating certificate status through CRL repositories; and
  - Adherence to this CPS and Aetna's Certificate Policy

- **Confidentiality**
  - Creation and signing of certificates binding end users to their public encryption key;
  - Creation and recovery of end entity confidential key pairs if required;

- Promulgating certificate status through CRL repositories; and
- Adherence to this CPS and GeoRoot's Certificate Policy.

1.1.4 Registration Authorities (RAs)

There may be one or more Registration Authorities associated with the Aetna GeoRoot CA. Either the CAs or RAs operating within the Aetna PKI service may perform identification and authentication requirements.

1.1.5 Repositories

The Aetna GeoRoot CA will have at least one certificate repository and one CRL repository, or one repository that holds certificates and CRLs. This may be the Microsoft Certificate Services internal store or an external store such as a database or LDAP accessible directory. The CRL and certificate repository should be publicly available in order to allow relying parties access to CRL and certificate data.

1.1.6 Subscribers

For the purposes of this CPS, a Subscriber is an entity that has been issued an SSL certificate.

Eligibility for a certificate is at the sole discretion of Aetna.

The number of subscribers is limited by the contract with Aetna for end user and SSL certificates.

1.1.7 Relying Parties

A Relying Party is an entity that relies on a certificate or information about the certificate that is issued by the Aetna GeoRoot CA.

1.1.8 Applicability

This CPS is applicable to all certificates issued by the Aetna GeoRoot CA. The practices described in this CPS apply to the issuance, use of the certificates and the revocation of certificates of Subscribers and Relying Parties of the Aetna GeoRoot CA.

1.1.9 Certificates issued by Aetna GeoRoot CA are:

Signature

Designed to be suitable for protecting the integrity and authentication of business transactions as well as providing non-repudiation.

Confidentiality

Designed to be suitable for certificate use such as encryption of information to facilitate the confidential transfer and storage of information.

1.2 Definitions

For the purposes of this CPS, all capitalized terms used herein shall have the meaning given to them in Section 8, Definitions, or elsewhere in this CPS.

1.3 Abbreviations

CA	Certification Authority
CN	Common Name
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DN	Distinguished Name
FIPS	Federal Information Processing Standard
IETF	Internet Engineering Task Force
ITU	International Telecommunications Union
LDAP	Light-Weight Directory Access Protocol
O	Organization
OCSP	On-line Certificate Status Protocol
OU	Organizational Unit
PKIX	Public Key Infrastructure X.509
RDN	Relative Distinguished Name
RFC	Request For Comment
SHA –1	Secure Hash Algorithm
SSL	Secure Sockets Layer
VPN	Virtual Private Network

1.4 Description and Use of Certificates

1. Aetna GeoRoot Certification Authority

Certificates issued by the Aetna GeoRoot Certification Authority are X.509 Certificates with SSL Extensions that chain to GeoTrust's trusted root and which facilitate secure

electronic commerce by providing limited authentication of Subjects and permitting SSL encrypted transactions between a Relying Party's browser and Aetna.

2. Operational Period of Certificates

Aetna's GeoRoot Certification Authority signed certificates will have an Operational Period of two years from the date of issuance, unless another time period or expiration date is specified on such Certificate, or unless the Certificate is revoked prior to the expiration of the Certificate's Operational Period.

If a Subscriber renews a Certificate within a specified period prior to expiration of an existing Certificate, Aetna may extend the Operational Period for the new Certificate by a specified number of days intended to give the Subscriber the approximate benefit of the remaining Operational Period of the existing Certificate. In addition, from time to time Aetna may extend the Operational Period of the Certificates it issues. The specific details of these extensions of the Operational Period will be provided to the Subscriber by information posted on the Aetna Web site, the enrollment form, and/or the Subscriber Agreement. The Operational Period for a Certificate will be stated in the Certificate.

3. Installation of Certificates

Certificates may not be installed on more than a single client at a time unless Subscriber has requested and Aetna has approved such a request during the enrollment process.

4. Technical Requirements of Certificates

In order to use a Certificate, the appropriate server software must support SSL.

2 GENERAL PROVISIONS

2.1 Obligations

1. Aetna Obligations

Aetna will:

(i) Issue Certificates in accordance with this CPS;

(ii) Perform limited authentication of Subscribers as described in this CPS;

(iii) Revoke Certificates as described in this CPS; and

(iv) Perform any other functions which are described within this CPS.

2. Subscriber Obligations

Subscriber will submit truthful information about itself and its business entity, domain ownership and contacts, as applicable. Subscribers will at all times abide by this CPS. The Subscriber is solely responsible for the protection of its Private Key and will immediately request revocation of a Certificate if the related Private Key is compromised. The Subscriber will only use the certificate issued by the Aetna GeoRoot Certificate Authority for purposes of negotiating SSL sessions.

3. Relying Party Obligations

Relying Parties must verify that the Certificate is valid by examining the Certificate Revocation List before initiating a transaction involving such Certificate. Aetna does not accept responsibility for reliance on a fraudulently obtained Certificate or a Certificate that is on the CRL.

2.2 Fees

1. Issuance, Management, and Renewal Fees

Aetna will not charge Subscribers for the issuance, management, and renewal of Certificates.

Certificate Access Fees

Aetna does not charge a fee as a condition of making a Certificate available in a repository or otherwise making Certificates available to Relying Parties.

2. Revocation or Status Information Fees

Aetna does not charge a fee as a condition of making the CRL available in a repository or otherwise available to Relying Parties. Aetna may, however, charge a fee for providing customized CRLs, OCSP services, or other value-added revocation and status information services. Aetna does not permit access to revocation information, Certificate status information, or time stamping in its repository by third parties that provide products or services that utilize such Certificate status information without Aetna's prior express consent.

3. Fees for Other Services Such as Policy Information

Aetna does not charge a fee for access to this CPS.

4. Reissue Policy

Request to Aetna or request to reissue of a Certificate based upon a prior Certificate Signing Request previously provided to Aetna by the Subscriber.

Aetna will not revoke a Certificate previously issued following a reissue request. A request for reissue of a Certificate will not be treated as a request by the Subscriber for revocation of a Certificate previously issued by Aetna unless the Subscriber follows the procedures for requesting revocation as stated at Section III.I. of this CPS.

2.3 Compliance

Aetna will adhere to the following guidelines:

- Maintain an accurate Certificate Revocation List (CRL) for all company issued certificates;
- GeoTrust may request a statement of compliance, or may perform an audit;
- All domains must be owned by Aetna Inc.;
- The certificates can be installed on as many servers as needed by Aetna Inc.;
- The SSL certificates must include the standard set of X.509 extensions;

The following guidelines apply to issuance of SSL certificates:

- Certificates can be issued to Aetna employees and company partners only for use and may not be resold or provided to users with no affiliation with Aetna Inc.;
- The certificates must include the standard set of X.509 extensions;

Aetna may also perform periodic internal security audits by trained and qualified security personnel according to Aetna's security policies and procedures. Results of the periodic audits are presented to Aetna's PKI team and upper management with a description of any deficiencies noted and corrective actions taken.

2.4 Limited Warranty/Disclaimer

Aetna provides the following limited warranty at the time of Certificate issuance: (i) it issued the Certificate substantially in compliance with this CPS; (ii) the information contained within the Certificate accurately reflects the information provided to Aetna by the Applicant in all material respects; and (iii) it has taken reasonable steps to verify that the information within the Certificate is accurate. The nature of the steps Aetna takes to verify the information contained in a Certificate is set forth in Section III of this CPS.

EXCEPT FOR THE LIMITED WARRANTY DESCRIBED ABOVE, AETNA EXPRESSLY DISCLAIMS AND MAKES NO REPRESENTATION, WARRANTY OR COVENANT OF ANY KIND, WHETHER EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, WITH RESPECT TO THIS CPS OR ANY CERTIFICATE ISSUED HEREUNDER, INCLUDING WITHOUT LIMITATION, ALL WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE OR USE OF A CERTIFICATE OR ANY SERVICE (INCLUDING, WITHOUT LIMITATION, ANY SUPPORT SERVICES) PROVIDED BY AETNA AS DESCRIBED HEREIN, AND ALL WARRANTIES, REPRESENTATIONS,

CONDITIONS, UNDERTAKINGS, TERMS AND OBLIGATIONS IMPLIED BY STATUTE OR COMMON LAW, TRADE USAGE, COURSE OF DEALING OR OTHERWISE ARE HEREBY EXCLUDED TO THE FULLEST EXTENT PERMITTED BY LAW. EXCEPT FOR THE LIMITED WARRANTY DESCRIBED ABOVE, AETNA FURTHER DISCLAIMS AND MAKES NO REPRESENTATION, WARRANTY OR COVENANT OF ANY KIND, WHETHER EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, TO ANY APPLICANT, SUBSCRIBER OR ANY RELYING PARTY THAT (A) THE SUBSCRIBER TO WHICH IT HAS ISSUED A CERTIFICATE IS IN THE FACT THE PERSON, ENTITY OR ORGANIZATION IT CLAIMS TO HAVE BEEN (B) A SUBSCRIBER IS IN FACT THE PERSON, ENTITY OR ORGANIZATION LISTED IN THE CERTIFICATE, OR (C) THAT THE INFORMATION CONTAINED IN THE CERTIFICATES OR IN ANY CERTIFICATE STATUS MECHANISM COMPILED, PUBLISHED OR OTHERWISE DISSEMINATED BY AETNA, OR THE RESULTS OF ANY CRYPTOGRAPHIC METHOD IMPLEMENTED IN CONNECTION WITH THE CERTIFICATES IS ACCURATE, AUTHENTIC, COMPLETE OR RELIABLE.

IT IS AGREED AND ACKNOWLEDGED THAT APPLICANTS ARE LIABLE FOR ANY MISREPRESENTATIONS MADE TO AETNA AND RELIED UPON BY A RELYING PARTY. AETNA DOES NOT WARRANT OR GUARANTEE UNDER ANY CIRCUMSTANCES THE "NON-REPUDIATION" BY A SUBSCRIBER AND/OR RELYING PARTY OF ANY TRANSACTION ENTERED INTO BY THE SUBSCRIBER AND/OR RELYING PARTY INVOLVING THE USE OF OR RELIANCE UPON A CERTIFICATE.

IT IS UNDERSTOOD AND AGREED UPON BY SUBSCRIBERS AND RELYING PARTIES THAT IN USING AND/OR RELYING UPON A CERTIFICATE THEY ARE SOLELY RESPONSIBLE FOR THEIR RELIANCE UPON THAT CERTIFICATE AND THAT SUCH PARTIES MUST CONSIDER THE FACTS, CIRCUMSTANCES AND CONTEXT SURROUNDING THE TRANSACTION IN WHICH THE CERTIFICATE IS USED IN DETERMINING SUCH RELIANCE.

THE SUBSCRIBERS AND RELYING PARTIES AGREE AND ACKNOWLEDGE THAT CERTIFICATES HAVE A LIMITED OPERATIONAL PERIOD AND MAY BE REVOKED AT ANY TIME. SUBSCRIBERS AND RELYING PARTIES ARE UNDER AN OBLIGATION TO VERIFY WHETHER A CERTIFICATE IS EXPIRED OR HAS BEEN REVOKED. AETNA HEREBY DISCLAIMS ANY AND ALL LIABILITY TO SUBSCRIBERS AND RELYING PARTIES WHO DO NOT FOLLOW SUCH PROCEDURES. MORE INFORMATION ABOUT THE SITUATIONS IN WHICH A CERTIFICATE MAY BE REVOKED CAN BE FOUND IN SECTION III(I) OF THIS CPS.

Aetna provides no warranties with respect to another party's software, hardware or telecommunications or networking equipment utilized in connection with the use, issuance, revocation or management of Certificates or providing other services (including, without limitation, any support services) with respect to this CPS. Applicants, Subscribers and Relying Parties agree and acknowledge that Aetna is not responsible or liable for any misrepresentations or incomplete representations of

Certificates or any information contained therein caused by another party's application software or graphical user interfaces. The cryptographic key-generation technology used by Applicants, Subscribers and Relying Parties in conjunction with the Certificates may or may not be subject to the intellectual property rights of third-parties. It is the responsibility of Applicants, Subscribers and Relying Parties to ensure that they are using technology which is properly licensed or to otherwise obtain the right to use such technology.

2.5 Limitation on Liability

EXCEPT TO THE EXTENT CAUSED BY AETNA'S WILLFUL MISCONDUCT, IN NO EVENT SHALL THE CUMULATIVE LIABILITY OF AETNA TO APPLICANTS, SUBSCRIBER AND/OR ANY RELYING PARTY FOR ALL CLAIMS RELATED TO THE INSTALLATION OF, USE OF OR RELIANCE UPON A CERTIFICATE OR FOR THE SERVICES PROVIDED HEREUNDER INCLUDING WITHOUT LIMITATION ANY CAUSE OF ACTION SOUNDING IN CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY, FOR BREACH OF A STATUTORY DUTY OR IN ANY OTHER WAY EXCEED FIVE THOUSAND U.S. DOLLARS ($5,000.00).

AETNA SHALL NOT BE LIABLE IN CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY, FOR BREACH OF A STATUTORY DUTY OR IN ANY OTHER WAY (EVEN IF AETNA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES) FOR:

> (I) ANY ECONOMIC LOSS (INCLUDING, WITHOUT LIMITATION, LOSS OF REVENUES, PROFITS, CONTRACTS, BUSINESS OR ANTICIPATED SAVINGS); (II) TO THE EXTENT ALLOWED BY APPLICABLE LAW, ANY LOSS OR DAMAGE RESULTING FROM DEATH OR INJURY OF SUBSCRIBER AND/OR ANY RELYING PARTY OR ANYONE ELSE; (III) ANY LOSS OF GOODWILL OR REPUTATION; OR (IV) ANY OTHER INDIRECT, CONSEQUENTIAL, INCIDENTAL, MULTIPLE, SPECIAL, PUNITIVE, EXEMPLARY DAMAGES

IN ANY CASE WHETHER OR NOT SUCH LOSSES OR DAMAGES WERE WITHIN THE CONTEMPLATION OF THE PARTIES AT THE TIME OF THE APPLICATION FOR, INSTALLATION OF, USE OF OR RELIANCE ON THE CERTIFICATE, OR AROSE OUT OF ANY OTHER MATTER OR SERVICES (INCLUDING, WITHOUT LIMITATION, ANY SUPPORT SERVICES) UNDER THIS CPS OR WITH REGARD TO THE USE OF OR RELIANCE ON THE CERTIFICATE.

BECAUSE SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, THE ABOVE EXCLUSIONS OF INCIDENTAL AND CONSEQUENTIAL DAMAGES MAY NOT APPLY TO AN APPLICANT, SUBSCRIBER AND/OR A RELYING PARTY BUT SHALL BE GIVEN EFFECT TO THE FULL EXTENT PERMITTED BY LAW.

THE FOREGOING LIMITATIONS OF LIABILITY SHALL APPLY ON A CERTIFICATE-BY-CERTIFICATE BASIS, REGARDLESS OF THE NUMBER OF TRANSACTIONS OR CLAIMS

RELATED TO EACH CERTIFICATE, AND SHALL BE APPORTIONED FIRST TO THE EARLIER CLAIMS TO ACHIEVE FINAL RESOLUTION.

In no event will Aetna be liable for any damages to Applicants, Subscribers, Relying Parties or any other party arising out of or related to the use or misuse of, or reliance on any Certificate issued under this CPS that:

(i) has expired or been revoked;

(ii) has been used for any purpose other than as set forth in the CPS (See Section I(c) for more detail);

(iii) has been tampered with;

(iv) with respect to which the Key Pair underlying such Certificate or the cryptography algorithm used to generate such Certificate's Key Pair, has been Compromised by the action of any party other than Aetna (including without limitation the Subscriber or Relying Party); or

(v) is the subject of misrepresentations or other misleading acts or omissions of any other party, including but not limited to Applicants, Subscribers and Relying Parties.

In no event shall Aetna be liable to the Applicant, Subscriber, Relying Party or other party for damages arising out of any claim that a Certificate infringes any patent, trademark, copyright, trade secret or other intellectual property right of any party.

2.6 Force Majeure

Aetna shall not be liable for any default or delay in the performance of its obligations hereunder to the extent and while such default or delay is caused, directly or indirectly, by fire, flood, earthquake, elements of nature or acts of God, acts of war, terrorism, riots, civil disorders, rebellions or revolutions in the United States, strikes, lockouts, or labor difficulties or any other similar cause beyond the reasonable control of Aetna.

2.7 Financial Responsibility

1. Fiduciary Relationships

Aetna is not an agent, fiduciary, trustee, or other representative of the Applicant or Subscriber and the relationship between Aetna and the Applicant and the Subscriber is not that of an agent and a principal. Aetna makes no representation to the contrary, either explicitly, implicitly, by appearance or otherwise. Neither the Applicant nor the Subscriber has any authority to bind Aetna by contract or otherwise, to any obligation.

2. Indemnification by Applicant and Subscriber

Unless otherwise set forth in this CPS and/or Subscriber Agreement, Applicant and Subscriber, as applicable, hereby agrees to indemnify and hold Aetna (including, but not limited to, its officers, directors, employees, agents, successors and assigns) harmless from any claims, actions, or demands that are caused by the use or publication of a Certificate and that arises from

(a) Any false or misleading statement of fact by the Applicant (or any person acting on the behalf of the Applicant)

(b) Any failure by the Applicant or the Subscriber to disclose a material fact, if such omission was made negligibly or with the intent to deceive;

(c) Any failure on the part of the Subscriber to protect its Private Key and Certificate or to take the precautions necessary to prevent the Compromise, disclosure, loss, modification or unauthorized use of the Private Key or Certificate; or

(d) Any failure on the part of the Subscriber to promptly notify Aetna, as the case may be, of the Compromise, disclosure, loss, modification or unauthorized use of the Private Key or Certificate once the Subscriber has constructive or actual notice of such event.

2.8 Interpretation & Enforcement

1. Governing Law

The enforceability, construction, interpretation, and validity of this CPS and any Certificates issued by Aetna shall be governed by the substantive laws of the State of

Connecticut, United States of America, excluding

(i) the conflicts of law provisions thereof and

(ii) The United Nations Convention on Contracts for the International Sale of Goods.

2. Dispute Resolution Procedures

Any dispute, controversy or claim arising under, in connection with or relating to this CPS or any Certificate issued by Aetna shall be subject to and settled finally by binding arbitration in accordance with the Arbitration Rules of the American Arbitration Association (AAA). All arbitration proceedings shall be held in Hartford, CT. There shall be one arbitrator appointed by the AAA who shall exhibit a reasonable familiarity with the issues involved or presented in such dispute, controversy or claim. The award of the arbitrator shall be binding and final upon all parties, and judgment on the award may be entered by any court having proper jurisdiction thereof. This CPS and the rights and obligations of the parties hereunder and under any Certificate issued by Aetna shall remain in full force and effect pending the outcome and award in any arbitration proceeding hereunder. In any arbitration arising hereunder, each party to the preceding shall be responsible for its own costs incurred in connection with the arbitration proceedings, unless the arbitrator determines that the prevailing party is entitled to an award of all or a portion of such costs, including reasonable attorneys fees actually incurred.

3. Conflict of Provisions

This CPS represents the entire agreement between any Subscriber (including the Subscriber Agreement, if any) or Relying Party and Aetna and supersedes any and all prior understandings and representations pertaining to its subject matter. In the event, however, of a conflict between this CPS and any other express agreement a

Subscriber has with Aetna with respect to a Certificate, including but not limited to a Subscriber Agreement, such other agreement shall take precedence.

4. Severability

If any provision of this CPS shall be held to be invalid, illegal, or unenforceable, the validity, legality, or enforceability of the remainder of this CPS shall not in any way be affected or impaired hereby.

2.9 Repository and CRL

With regard to Aetna GeoRoot Certification Authority (including those provided through the Enterprise SSL service), Aetna shall operate a CRL that will be available to both Subscribers and Relying Parties. Aetna shall post the CRL online at least weekly in a DER format except as otherwise provided in Aetna's Business Continuity Plan. Each CRL is signed by the issuing Aetna CA. The procedures for revocation are as stated elsewhere in this CPS.

Aetna retains copies of all Certificates for the life of the CA, but does not archive or retain expired or superseded CRLs. Aetna does not provide other online status mechanisms (e.g., OCSP) for checking certificate status requests.

2.10 Confidentiality Policy

1. Individual Subscriber Information

Except as provided herein, certain information regarding Subscribers that is submitted on enrollment forms for Certificates will be kept confidential by Aetna (such as contact information for individuals) and Aetna shall not release such information without the prior consent of the Subscriber. Notwithstanding the foregoing, Aetna may make such information available

(a) to courts, law enforcement agencies or other third parties (including release in response to civil discovery) upon receipt of a court order or subpoena or upon the advice of Aetna's legal counsel,

(b) to law enforcement officials and others for the purpose of investigating suspected fraud, misrepresentation, unauthorized access, or potential illegal activity by the Subscriber in the opinion of Aetna and

(c) to third parties as may be necessary for Aetna to perform its responsibilities under this Agreement. The foregoing confidentiality obligation shall not apply, however, to information appearing on Certificates, information relating to Certificate revocation, or to information regarding Subscribers that is already in the possession of or separately acquired by Aetna.

2. Aggregate Subscriber Information

Notwithstanding the previous Section, Aetna may disclose Subscriber information on an aggregate basis, and the Subscriber hereby grants to Aetna a license to do so, including the right to modify the aggregated Subscriber information and to permit third parties to perform such functions on its behalf. Aetna shall not disclose to any third party any personally identifiable information about any Subscriber that Aetna obtains in its performance of services hereunder.

2.11 Waiver

A failure or delay in exercising any right or remedy hereunder shall not operate as a waiver of that right or remedy, nor shall any single or partial exercise of any right or remedy preclude any other or further exercise thereof or the exercise of any other right or remedy.

2.12 Survival

The following sections shall survive, along with all definitions required thereby: Sections I, II, and VIII.

2.13 Export

Subscribers and Relying Parties acknowledge and agree to use Certificates in compliance with all applicable laws and regulations, including without limitation U.S. export laws and regulations. Aetna may refuse to issue or may revoke Certificates if in the reasonable opinion of Aetna such issuance or the continued use of such Certificates would violate applicable laws and regulations.

3 OPERATIONAL REQUIREMENTS

3.1 Application Requirements

An Applicant for an Aetna GeoRoot Certification Authority Certificate shall complete an Aetna GeoRoot Certification Authority Certificate enrollment form in a form prescribed by Aetna. All enrollment forms are subject to review, approval and acceptance by Aetna. All Applicants are required to include a Domain Name within the GeoRoot SSL Certificate enrollment form. Aetna verifies the authority of the Subscriber to request a Certificate. Aetna authenticates the user against Active Directory (and checks generally for errors and omissions relevant to the authentication steps taken). Aetna also verifies the accuracy of the information contained in the Subscriber's Certificate request and checks for errors and omissions.

3.2 Certificate Information

1. Organizational Name

Aetna will insert the domain name in the Organization field for all certificates issued by the Aetna GeoRoot Certification Authority.

3.3 Procedure for Processing Certificate Applications

1. Enrollment Form

Subscribers submit their Public Key to Aetna for certification electronically through the use of a PKCS#10 Certificate Signing Request (CSR) or other package digitally signed by the Subscriber's Private Key in a session secured by Secure Sockets Layer (SSL). At a minimum, the Subscriber must provide the following data in or with the CSR: Common Name, Organization, City, State, and Country. The following additional information may be required on the enrollment form: the names, e-mail addresses, and telephone numbers for the Administrative, Technical, Support, and Billing points of contact. Aetna reserves the right to use subcontractors or other third parties to assist in the performance of its operational requirements or any other obligation under this CPS.

3.4 Application Issues

At certain times during the application process in which Aetna is not able to verify information in an enrollment form, a customer service representative may be assigned to the applicant to facilitate the completion of the application process. Otherwise, the applicant may be required to correct its associated information with third parties and re-submit its enrollment form for a Certificate.

3.5 Certificate Delivery

If Aetna finds that the applicant's enrollment form was sufficiently verified, then the applicant's Certificate will be signed by Aetna. Upon signing the applicant's Certificate,

Aetna will attach such Certificate to an e-mail and send such e-mail to the appropriate contacts or make the Certificate available via the Application Programming Interface (API). Aetna, in its sole discretion, may provide technical or customer support to the applicants/Subscribers. Aetna does not distribute Certificates via Integrated Circuit Cards (ICC) to Subscribers.

3.6 Certificate Acceptance

The applicant expressly indicates acceptance of a Certificate by using such Certificate.

3.7 Certificate Renewal and Rekey

Prior to the expiration of an existing Subscriber's Certificate, it is necessary for the Subscriber to obtain a new Certificate to maintain continuity of Certificate usage. Subscribers have the option of generating a new Key Pair to replace the expiring Key Pair (technically defined as "rekey") or of creating a new Certificate Signing Request for an existing Key Pair (technically defined as "renewal"), depending on their preferences and the capabilities and restrictions of the Subscriber's web server and web server key generation tools. For purposes of this CPS, both a "rekey" and "renewal" as defined above will be treated as a renewal Certificate.

Renewal Certificates are subject to the same authentication steps outlined in this CPS as apply to initial issuance of a Certificate. Expiring Certificates are not revoked by Aetna upon issuance of the renewal Certificate.

The Subscriber must pay the fees and comply with the other terms and conditions for renewal as presented on Aetna's Web site.

3.8 Certificate Expiration

Aetna will attempt to notify all Subscribers of the expiration date of their Certificate. Notifications will generally be by e-mail message to the contacts listed in the enrollment form submitted by Subscriber, and will likely occur periodically during the 90 day period prior to the expiration date and the 14 day period following the expiration date. If Subscriber's enrollment form was submitted by another party on Subscriber's behalf, Aetna likely will not send expiration notices to that party.

3.9 Certificate Revocation

1. Circumstances For Revocation

Certificate revocation is the process by which Aetna prematurely ends the Operational Period of a Certificate by posting the serial number of the Certificate to a Certificate Revocation List.

A Subscriber shall inform Aetna and promptly request revocation of a Certificate:

- whenever any of the information on the Certificate changes or becomes obsolete; or

- whenever the Private Key, or the media holding the Private Key, associated with the Certificate is Compromised; or
- upon a change in the ownership of a Subscriber's web server.

Subscriber shall state the reason(s) for requesting revocation upon submitting the request.

Aetna shall revoke a Certificate:

- upon request of a Subscriber as described above;
- in the event of Compromise of Aetna's Private Key used to sign a Certificate;
- upon the Subscriber's breach of either this CPS or Subscriber Agreement;
- if Aetna determines that the Certificate was not properly issued; or
- in the event the Certificate is installed on more than a single server at a time without permission of Aetna.

If Aetna initiates revocation of a Certificate, Aetna shall notify the contact provided by Subscriber by e-mail message of the revocation and the reasons why. In the event that Aetna ceases operations, all Certificates issued by Aetna shall be revoked prior to the date that Aetna ceases operations, and Aetna shall notify the contact provided by Subscriber by e-mail message of the revocation and the reasons why.

A refund and/or reissue request by a Subscriber will not be treated as a request for revocation of a Certificate under this subsection unless the Subscriber specifically requests revocation of the Certificate.

2. Who Can Request Revocation

The only persons permitted to request revocation of a Certificate issued by Aetna are the Subscriber (including designated representatives or the contact.

3. Procedure For Revocation Request

To request revocation, a Subscriber must contact Aetna, either by e-mail message, a national/regional postal service, facsimile, or overnight courier, and specifically request “revocation” (using that term) of a particular Certificate identified by the Subscriber. Upon receipt of a revocation request, Aetna will seek confirmation of the request by e-mail message to the person requesting revocation. The message will state that, upon confirmation of the revocation request, Aetna will revoke the Certificate and that posting the revocation to the appropriate CRL will constitute notice to the Subscriber that the Certificate has been revoked. Aetna will require a confirming e-mail message back from either the contact authorizing revocation (or by other means of confirmation acceptable to Aetna). Upon receipt of the confirming e-mail message, Aetna will revoke the Certificate and the revocation will be posted to the appropriate CRL. Notification will be sent to the subject of the Certificate and the subject’s designated contacts. There is no grace period available to the Subscriber prior to revocation, and Aetna shall respond to the revocation request within the next business day and post the revocation to the next published CRL.

In the event of Compromise of Aetna's Private Key used to sign a Certificate, Aetna will send an e-mail message as soon as practicable to all Subscribers with Certificates issued off the Private Key stating that the Certificates will be revoked by the next business day and that posting the revocation to the appropriate CRL will constitute notice to the Subscriber that the Certificate has been revoked.

3.10 Certificate Suspension

Aetna does not support Certificate suspension for the Certificates. Aetna may revoke a certificate.

3.11 Key Management

Aetna may provide Subscriber Private Key protection or other Subscriber key management services in connection with its Certificates.

3.12 Subscriber Key Pair Generation

Aetna may provide Subscriber Key Pair generation or Subscriber Private Key protection for the Certificates.

3.13 Records Archival

Aetna shall maintain and archive records relating to the issuance of the Certificates for three (3) years following the issuance of the applicable Certificate.

3.14 CA Termination

In the event that it is necessary for Aetna or its CAs to cease operation, Aetna makes a commercially reasonable effort to notify Subscribers, Relying Parties, and other affected entities of such termination in advance of the CA termination. Where CA termination is required, Aetna will develop a termination plan to minimize disruption to Subscribers and Relying Parties. Such termination plans may address the following, as applicable:

- Provision of notice to parties affected by the termination, such as Subscribers and Relying Parties, informing them of the status of the CA,
- Handling the cost of such notice,
- The revocation of the Certificate issued to the CA by Aetna,
- The preservation of the CA’s archives and records for the time periods required in this CPS,
- The continuation of Subscriber and customer support services,
- The continuation of revocation services, such as the issuance of CRLs,
- The revocation of unexpired, unrevoked Certificates of Subscribers and subordinate CAs, if necessary,

- The issuance of replacement Certificates by a successor CA,
- Disposition of the CA's Private Key and the hardware tokens containing such Private Key,
- Provisions needed for the transition of the CA's services to a successor CA, and
- The identity of the custodian of Aetna's CA and RA archival records. Unless a different custodian is indicated through notice to Subscribers and Relying Parties, the Registered Agent for Aetna, Inc., shall be the custodian.

4 PHYSICAL SECURITY CONTROLS

4.1 Site Location and Construction

Aetna's CA operations are conducted within Aetna's facilities in Middletown, CT that meet GeoTrust and Industry best practices audit requirements. All Aetna CA operations are conducted within a physically protected environment designed to deter, prevent, and detect covert or overt penetration.

Aetna's CAs are physically located in a highly secure facility that includes the following:

- Electronic control access systems
- Alarmed doors and video monitoring
- Security logging and audits
- Proximity card access for specially approved employees with defined levels of management approval required

4.2 Physical Access Controls

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.

4.3 Power and Air Conditioning

Aetna's CA facility is equipped with primary and backup:

- Power systems to ensure continuous, uninterrupted access to electric power and
- Heating/ventilation/air conditioning systems to control temperature and relative humidity.

4.4 Water Exposures

The Aetna CA facility is located above ground on a raised floor and is not susceptible to flooding or other forms of water damage. Aetna has taken reasonable precautions to minimize the impact of water exposure to Aetna systems.

4.5 Fire Prevention and Protection

The fire detection system in Aetna CA facility tests air health and looks for certain signatures of possible fire conditions in the air. In addition, the Aetna CA facility has a pre-action water suppression system. When temperatures above 300 degrees are detected, the effected sprinkler head will release water on the area where the temperature rise is detected.

4.6 Media Storage

All media containing production software and data, audit, archive, or backup information is stored within multiple Aetna facilities in TL-30 rated safes with appropriate physical and logical access controls designed to limit access to authorized personnel and protect such media from accidental damage.

4.7 Waste Disposal

Sensitive documents and materials are shredded before disposal. Media used to collect or transmit sensitive information are rendered unreadable before disposal. Cryptographic devices are physically destroyed or zeroized in accordance the manufacturers' guidance prior to disposal. Other waste is disposed of in accordance with Aetna's normal waste disposal requirements.

4.8 Off-Site Backup

Aetna performs routine backups of critical system data, audit log data, and other sensitive information. Critical CA facility backup media are stored in a physically secure manner at an off-site facility.

5 TECHNICAL SECURITY CONTROLS

5.1 CA Key Pair

CA Key Pair generation is performed by multiple trained and trusted individuals using secure systems and processes that provide for the security and required cryptographic strength for the keys that are generated. All CA Key Pairs are generated in pre-planned key generation ceremonies in accordance with the requirements of Aetna security and audit requirements guidelines. The activities performed in each key generation ceremony are recorded, dated and signed by all individuals involved. These records are kept for audit and tracking purposes for a length of time deemed appropriate by Aetna management.

Certificates are issued off the Microsoft Certificate Authority CA.

The cryptographic modules used for key generation and storage meet the requirements of FIPS 140-1 level 3. Cryptographic module support is provided through the use of Hardware Security Modules. The Root Keys for each CA Certificate were generated and are stored in hardware and are backed up but not escrowed. The Root Keys are maintained under m of n multiperson control.

The Root Keys for each of the CA Certificates may be used for Certificate signing, CRL signing, and off-line CRL signing.

Aetna makes the CA Certificates available to Subscribers and Relying Parties through their inclusion in Microsoft and Netscape web browser software. For specific applications, Aetna's Public Keys are provided by the application vendors through the applications' root stores.

Aetna generally provides the full certificate chain (including the issuing CA Certificate and any CA Certificates in the chain) to the Subscriber upon Certificate issuance. Aetna CA Certificates may also be downloaded from the Aetna Resource Web site at http://crl.aetna.com.

There are no restrictions on the purposes for which the CA Key Pair may be used.

Aetna CA Key Pairs are maintained in a trusted and highly secured environment with backup and key recovery procedures. In the event of the Compromise of one or more of the Aetna Root Key(s) (including the CA Certificates), Aetna shall promptly notify all Subscribers via e-mail and notify Relying Parties and others via the CRL and additional notice posted at http://crl.aetna.com, and shall revoke all Certificates issued with such Aetna Root Key(s).

When Aetna CA Key Pairs reach the end of their validity period, such CA Key Pairs will be archived for a period of at least 5 years. Archived CA Key Pairs will be securely stored using off-line media. Procedural controls will prevent archived CA Key Pairs from being returned to production use. Upon the end of the archive period, archived CA Private Keys will be securely destroyed.

Aetna CA Key Pairs are retired from service at the end of their respective maximum lifetimes as defined above, and so there is no key changeover. Certificates may be

renewed as long as the cumulative certified lifetime of the Certificate Key Pair does not exceed the maximum CA Key Pair lifetime. New CA Key Pairs will be generated as necessary, for example to replace CA Key Pairs that are being retired, to supplement existing, active Key Pairs and to support new services in accordance with this CPS.

5.2 Subscriber Key Pairs

Aetna uses either 1024-bit or 2048-bit for all certificate requests. All Aetna certificates will accommodate the use of domestic and international 128-bit strength browsers and web servers.

Generation of Subscriber Key Pairs is generally performed by the Subscriber, and may be generated in either hardware or software. For server Certificates, the Subscriber typically uses the key generation utility provided with the web server software. Aetna does not require any particular standard for the module used to generate the keys. Key pairs generated by the Subscriber for Certificates may be used for server authentication. There are no purposes for which Aetna restricts the use of the Subscriber key.

For X.509 Version 3 Certificates, Aetna generally populates the KeyUsage extension of Certificates in accordance with RFC 2459: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, January 1999.

5.3 Business Continuity Management Controls

Aetna has business continuity plans (BCP) to maintain or restore the Aetna CAs business operations in a reasonably timely manner following interruption to or failure of critical business processes. The BCP define the following time periods for acceptable system outage and recovery time:

1 Vet a Subscriber - 1 week

2 Issue a Certificate - 2 weeks

3 Publish a CRL - 2 weeks

4 Audit Vetting Procedures - 2 months

Backup copies of essential business and CA information are made routinely. In general, back-ups are performed daily on-site, weekly to an off-site location, and monthly to Aetna’s disaster recovery site, but may be performed less frequently in Aetna’s discretion according to production schedule requirements.

5.4 Event Logging

Aetna CA event journal data is archived both daily and monthly. Daily event journals are reviewed daily. Monthly event journals are reviewed monthly.

6 CERTIFICATE AND CRL PROFILE

6.1 Certificate Profile

Aetna Certificates conform to (a) ITU-T Recommendation X.509 Version 3 (1997): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, June 1997, and (b) RFC 2459: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, January 1999 ("RFC 2459"). Certificate extensions and their criticality, as well as cryptographic algorithm object identifiers, are populated according to the IETF RFC 2459 standards and recommendations. The name forms for Subscribers are enforced through Aetna's internal policies and the authentication steps described elsewhere in this CPS. Name constraint enforcement is not through the name constraint extension, but through the authentication steps followed and contractual limitations with each Subscriber. Aetna does not apply any specific Certificate Policy Object Identifier(s), but instead refers to the applicable CPS version and URL address. The policy constraints extensions and policy qualifiers syntax and semantics, when used, conform to the RFC 2459 standards.

6.2 CRL Profile

Aetna issued CRLs conform to all RFC 2459 standards and recommendations.

7 CPS ADMINISTRATION

7.1 CPS Authority

The authority administering this CPS is the Aetna PKI Policy Authority. Inquiries to Aetna's PKI Policy Authority should be addressed as follows:

Aetna, Inc. pkiadmin@Aetna.com

Aetna does not support a Certificate Policy (CP) for GeoRoot Certification Authority.

7.2 Contact Person

Address inquiries about the CPS to pkiadmin@Aetna.com

7.3 CPS Change Procedures

This CPS (and all amendments to this CPS) is subject to approval by the PKI Policy Authority. Aetna may change this CPS at any time without prior notice. The CPS and any amendments thereto is available through http://crl.aetna.com Amendments to this CPS will be evidenced by a new version number and date, except where the amendments are purely clerical.

8 DEFINITIONS

8.1 CA: Certification Authority.

Certificate: A record that, at a minimum: (a) identifies the CA issuing it; (b) names or otherwise identifies its Subscriber; (c) contains a Public Key that corresponds to a Private Key under the control of the Subscriber; (d) identifies its Operational Period; and (e) contains a Certificate serial number and is digitally signed by the CA. The term Certificate, as referred to in this CPS, means a Certificate issued by Aetna pursuant to this CPS.

Certificate Revocation List: A time-stamped list of revoked Certificates that has been digitally signed by the CA.

Certification Authority: An entity which issues Certificates and performs all of the functions associated with issuing such Certificates.

Compromise: Suspected or actual unauthorized disclosure, loss, loss of control over, or use of a Private Key associated with Certificate.

CRL: See Certificate Revocation List.

Extension: means to place additional information about a Certificate within a Certificate. The X.509 standard defines a set of Extensions that may be used in Certificates.

Aetna: Aetna, Inc.

Key Pair: Two mathematically related keys, having the following properties: (i) one key can be used to encrypt a message that can only be decrypted using the other key, and (ii) even knowing one key, it is computationally impractical to discover the other key.

Operational Period: A Certificate's period of validity. It typically begins on the date the Certificate is issued (or such later date as specified in the Certificate), and ends on the date and time it expires as noted in the Certificate unless the Certificate is revoked before its expiration.

Organization: The entity named or identified in a Certificate in the Organizational Name field that has either subscribed to Aetna's Enterprise SSL Service or purchased a Certificate.

Private Key: The key of a Key Pair used to create a digital signature. This key must be kept a secret.

Public Key: The key of a Key Pair used to verify a digital signature. The Public Key is made freely available to anyone who will receive digitally signed messages from the holder of the Key Pair. The Public Key is usually provided via a Certificate issued by Aetna. A Public Key is used to verify the digital signature of a message purportedly sent by the holder of the corresponding Private Key.1819

Relying Party: A recipient of a digitally signed message who relies on a Certificate to verify the digital signature on the message. Also, a recipient of a Certificate who relies on the information contained in the Certificate.

Root Key(s): The Private Key used by Aetna to sign the Certificates.

SSL: An industry standard protocol that uses public key cryptography for Internet security.

Subscriber: A person or entity who (1) is the subject named or identified in a Certificate issued to such person or entity, (2) holds a Private Key that corresponds to a Public Key listed in that Certificate, and (3) the person or entity to whom digitally signed messages verified by reference to such Certificate are to be attributed. For the purpose of this CPS, a person or entity who applies for a Certificate by the submission of an enrollment form is also referred to as a Subscriber.

"GeoRoot" : "GeoRoot" is an ideal solution that allows enterprises to retain full control over Registration Authority (RA) functions for the issuance of SSL certificates for domains and client certificates (x.509). "GeoRoot" is property of GeoTrust.

[v. 1.0]