

RSA[®] Root Signing Service Certificate Policy

Revision Date: June 7, 2007

Version: 3.0

Published By: RSA Security Inc.

Copyright © 2001, 2002, 2005, 2007 – RSA Security Inc. All rights reserved.

No part of this document may be reproduced, modified or distributed in any form or by any means, in whole or in part, or stored in a database or retrieval system, without prior written permission of RSA Security Inc.

BSAFE, RSA, the RSA logo, RSA Security and SecurID are either registered trademarks or trademarks of RSA Security Inc. in the United States and/or other countries.

All other trademarks mentioned herein are the property of their respective owners.

RSA, The Security Division of EMC² heretofore known as RSA Security Inc. shall be referenced in the text of the pages that follow as "RSA"

Revision History

Revision History

Version	Date	Author's initials	Description of changes
1.0	09/10/2001	MS	First release
1.01	10/16/2001	MS	Minor changes
1.02	10/16/2001	MS	Minor changes
1.03	11/22/2001	MS	Minor changes
1.04	12/13/2001	MS	Minor changes, moved paragraphs from section 2.1.1.2 to section 2.1.1.1 (provide notice)
1.04a	1/11/2002	MS	Added numeric OID
1.05	2/7/2002	MS	Changed RSA Root Signing CA to RSA Public Root CA v1 Changed section 6.2.2
1.06	2/28/2002	MS	Changed name from RSA Security Inc to RSA Security Holdings Inc., added "the" to the front of RSA KEON ROOT SIGNING SERVICE
1.07	4/5/2002	MS	Section 3.1.1 added UTF8String to last sentence to provide support for UTF8 in DN Section 3.1.5 Added sentences for Domain Name and Email Addresses to restrict use to authenticated owners
1.1	5/18/2005	RL	Incorporation of comments received from customer subscribers. Preparation for format change to new RFC 3647 standard.
2.0	6/10/2005	RL	Conversion to RFC 3647
2.1	9/15/2005	DF	Minor clarification to section 1.4
3.0	6/7/2007	DF	Incorporation of coverage for EV certificates and 2048 v3 RSA Root

Table of Contents

CERTIFICATE POLICY SUMMARY 1

 OVERVIEW 1

 INTRODUCTION..... 2

POLICY SPECIFICATION 4

1 INTRODUCTION 4

 1.1 OVERVIEW 4

 1.2 DOCUMENT NAME AND IDENTIFICATION 4

 1.3 PKI PARTICIPANTS..... 4

 1.3.1 Certification Authorities (CA) 4

 1.3.2 Registration Authorities (RA) 5

 1.3.3 Subscribers 5

 1.3.4 Relying parties 5

 1.3.5 Other participants..... 5

 1.4 CERTIFICATE USAGE 5

 1.4.1 Appropriate certificate uses 5

 1.4.2 Prohibited certificate uses..... 6

 1.5 POLICY ADMINISTRATION..... 6

 1.5.1 Organization administering the document 6

 1.5.2 Contact person..... 6

 1.5.3 Person determining CPS suitability for the policy 6

 1.5.4 CPS approval procedures..... 7

 1.6 DEFINITIONS AND ACRONYMS 7

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES..... 8

 2.1 REPOSITORIES 8

 2.2 PUBLICATION OF CERTIFICATION INFORMATION..... 8

 2.3 TIME OR FREQUENCY OF PUBLICATION 9

 2.4 ACCESS CONTROLS ON REPOSITORIES 9

3 IDENTIFICATION AND AUTHENTICATION..... 10

 3.1 NAMING 10

 3.1.1 Types of names 10

 3.1.2 Need for names to be meaningful..... 10

 3.1.3 Anonymity or pseudonymity of subscribers 10

 3.1.4 Rules for interpreting various name forms..... 10

 3.1.5 Uniqueness of names 10

 3.1.6 Recognition, authentication, and role of trademarks 10

 3.2 INITIAL IDENTITY VALIDATION 11

 3.2.1 Method to prove possession of private key 11

 3.2.2 Authentication of organization identity 11

 3.2.3 Authentication of individual identity..... 11

 3.2.4 Non-verified subscriber information 11

 3.2.5 Validation of authority 12

 3.2.6 Criteria for interoperation 12

 3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS 12

 3.3.1 Identification and authentication for routine re-key..... 12

 3.3.2 Identification and authentication for re-key after revocation 12

 3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST 13

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS..... 14

- 4.1 CERTIFICATE APPLICATION 14
 - 4.1.1 Who can submit a certificate application 14
 - 4.1.2 Enrollment process and responsibilities 14
- 4.2 CERTIFICATE APPLICATION PROCESSING 14
 - 4.2.1 Performing identification and authentication functions 15
 - 4.2.2 Approval or rejection of certificate applications 15
 - 4.2.3 Time to process certificate applications 15
- 4.3 CERTIFICATE ISSUANCE 15
 - 4.3.1 CA actions during certificate issuance 15
 - 4.3.2 Notification to subscriber by the CA of issuance of certificate 15
- 4.4 CERTIFICATE ACCEPTANCE 15
 - 4.4.1 Conduct constituting certificate acceptance 15
 - 4.4.2 Publication of the certificate by the CA 16
 - 4.4.3 Notification of certificate issuance by the CA to other entities 16
- 4.5 KEY PAIR AND CERTIFICATE USAGE 16
 - 4.5.1 Subscriber private key and certificate usage 16
 - 4.5.2 Relying party public key and certificate usage 16
- 4.6 CERTIFICATE RENEWAL 17
 - 4.6.1 Circumstance for certificate renewal 17
 - 4.6.2 Who may request renewal 17
 - 4.6.3 Processing certificate renewal requests 17
 - 4.6.4 Notification of new certificate issuance to subscriber 17
 - 4.6.5 Conduct constituting acceptance of a renewal certificate 17
 - 4.6.6 Publication of the renewal certificate by the CA 17
 - 4.6.7 Notification of certificate issuance by the CA to other entities 17
- 4.7 CERTIFICATE RE-KEY 18
 - 4.7.1 Circumstance for certificate re-key 18
 - 4.7.2 Who may request certification of a new public key 18
 - 4.7.3 Processing certificate re-keying requests 18
 - 4.7.4 Notification of new certificate issuance to subscriber 18
 - 4.7.5 Conduct constituting acceptance of a re-keyed certificate 18
 - 4.7.6 Publication of the re-keyed certificate by the CA 18
 - 4.7.7 Notification of certificate issuance by the CA to other entities 18
- 4.8 CERTIFICATE MODIFICATION 18
 - 4.8.1 Circumstance for certificate modification 18
 - 4.8.2 Who may request certificate modification 18
 - 4.8.3 Processing certificate modification requests 18
 - 4.8.4 Notification of new certificate issuance to subscriber 19
 - 4.8.5 Conduct constituting acceptance of modified certificate 19
 - 4.8.6 Publication of the modified certificate by the CA 19
 - 4.8.7 Notification of certificate issuance by the CA to other entities 19
- 4.9 CERTIFICATE REVOCATION AND SUSPENSION 19
 - 4.9.1 Circumstances for revocation 19
 - 4.9.2 Who can request revocation 20
 - 4.9.3 Procedure for revocation request 20
 - 4.9.4 Revocation request grace period 20
 - 4.9.5 Time within which CA must process the revocation request 20
 - 4.9.6 Revocation checking requirement for relying parties 20
 - 4.9.7 CRL issuance frequency 21
 - 4.9.8 Maximum latency for CRLs 21
 - 4.9.9 Online revocation/status checking availability 21
 - 4.9.10 Online revocation checking requirements 21
 - 4.9.11 Other forms of revocation advertisements available 21
 - 4.9.12 Special requirements re-key compromise 21
 - 4.9.13 Circumstances for suspension 21
 - 4.9.14 Who can request suspension 21

- 4.9.15 Procedure for suspension request..... 22
- 4.9.16 Limits on suspension period 22
- 4.10 CERTIFICATE STATUS SERVICES..... 22
 - 4.10.1 Operational characteristics 22
 - 4.10.2 Service availability 22
 - 4.10.3 Optional features..... 22
- 4.11 END OF SUBSCRIPTION..... 22
- 4.12 KEY ESCROW AND RECOVERY..... 22
 - 4.12.1 Key escrow and recovery policy and practices..... 22
 - 4.12.2 Session key encapsulation and recovery policy and practices 22
- 5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS 23**
 - 5.1 PHYSICAL CONTROLS..... 23
 - 5.1.1 Site location and construction..... 23
 - 5.1.2 Physical access 24
 - 5.1.3 Power and air conditioning 24
 - 5.1.4 Water exposures..... 24
 - 5.1.5 Fire prevention and protection 24
 - 5.1.6 Media storage 24
 - 5.1.7 Waste disposal..... 24
 - 5.1.8 Off-site backup..... 24
 - 5.2 PROCEDURAL CONTROLS 24
 - 5.2.1 Trusted roles 24
 - 5.2.2 Number of persons required per task 25
 - 5.2.3 Identification and authentication for each role 25
 - 5.2.4 Roles requiring separation of duties 25
 - 5.3 PERSONNEL CONTROLS 26
 - 5.3.1 Qualifications, experience, and clearance requirements..... 26
 - 5.3.2 Background check procedures 26
 - 5.3.3 Training requirements 26
 - 5.3.4 Retraining frequency and requirements..... 26
 - 5.3.5 Job rotation frequency and sequence..... 26
 - 5.3.6 Sanctions for unauthorized actions..... 26
 - 5.3.7 Independent contractor requirements..... 27
 - 5.3.8 Documentation supplied to personnel 27
 - 5.4 AUDIT LOGGING PROCEDURES..... 28
 - 5.4.1 Types of events recorded 28
 - 5.4.2 Frequency of processing log..... 28
 - 5.4.3 Retention period for audit log..... 28
 - 5.4.4 Protection of audit log 28
 - 5.4.5 Audit log backup procedures 28
 - 5.4.6 Audit collection system (internal vs. external) 28
 - 5.4.7 Notification to event-causing subject 28
 - 5.4.8 Vulnerability assessments 28
 - 5.5 RECORDS ARCHIVAL 29
 - 5.5.1 Types of records archived 29
 - 5.5.2 Retention period for archive..... 29
 - 5.5.3 Protection of archive 29
 - 5.5.4 Archive backup procedures 29
 - 5.5.5 Requirements for time-stamping of records 29
 - 5.5.6 Archive collection system (internal or external) 29
 - 5.5.7 Procedures to obtain and verify archive information 29
 - 5.6 KEY CHANGEOVER..... 29
 - 5.7 COMPROMISE AND DISASTER RECOVERY 30
 - 5.7.1 Incident and compromise handling procedures..... 30
 - 5.7.2 Computing resources, software, and/or data are corrupted 30

- 5.7.3 Entity private key compromise procedures..... 30
- 5.7.4 Business continuity capabilities after a disaster 30
- 5.8 CA OR RA TERMINATION..... 31
- 6 TECHNICAL SECURITY CONTROLS 32**
- 6.1 KEY PAIR GENERATION AND INSTALLATION 32
 - 6.1.1 Key pair generation..... 32
 - 6.1.2 Private Key delivery to subscriber 32
 - 6.1.3 Public key delivery to certificate issuer 32
 - 6.1.4 CA public key delivery to relying parties 32
 - 6.1.5 Key sizes..... 32
 - 6.1.6 Public key parameters generation and quality checking 32
 - 6.1.7 Key usage purposes (as per X.509 v3 key usage field) 32
- 6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS..... 33
 - 6.2.1 Cryptographic module standards and controls 33
 - 6.2.2 Private Key (n out of m) multi-person control 33
 - 6.2.3 Private Key escrow 33
 - 6.2.4 Private Key backup 34
 - 6.2.5 Private Key archival 34
 - 6.2.6 Private Key transfer into or from a cryptographic module 34
 - 6.2.7 Private Key storage on cryptographic module 34
 - 6.2.8 Method of activating private key 34
 - 6.2.9 Method of deactivating private key 34
 - 6.2.10 Method of destroying private key 34
 - 6.2.11 Cryptographic Module Rating 34
- 6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT 35
 - 6.3.1 Public key archival 35
 - 6.3.2 Certificate operational periods and key pair usage periods..... 35
- 6.4 ACTIVATION DATA 35
 - 6.4.1 Activation data generation and installation 35
 - 6.4.2 Activation data protection 35
 - 6.4.3 Other aspects of activation data 35
- 6.5 COMPUTER SECURITY CONTROLS 35
 - 6.5.1 Specific computer security technical requirements 35
 - 6.5.2 Computer security rating..... 35
- 6.6 LIFE CYCLE TECHNICAL CONTROLS 36
 - 6.6.1 System development controls..... 36
 - 6.6.2 Security management controls 36
 - 6.6.3 Life cycle security controls..... 36
- 6.7 NETWORK SECURITY CONTROLS..... 36
- 6.8 TIME-STAMPING..... 36
- 7 CERTIFICATE, CRL, AND OCSP PROFILES 37**
- 7.1 CERTIFICATE PROFILE..... 37
 - 7.1.1 Version number(s) 37
 - 7.1.2 Certificate extensions..... 37
 - 7.1.3 Algorithm object identifiers..... 37
 - 7.1.4 Name forms 37
 - 7.1.5 Name constraints 37
 - 7.1.6 Certificate policy object identifier 37
 - 7.1.7 Usage of Policy Constraints extension 37
 - 7.1.8 Policy qualifiers syntax and semantics 37
 - 7.1.9 Processing semantics for the critical Certificate Policies extension 37
- 7.2 CRL PROFILE 38
 - 7.2.1 Version number(s) 38
 - 7.2.2 CRL and CRL entry extensions 38

- 7.3 OCSP PROFILE 38
 - 7.3.1 Version number(s) 38
 - 7.3.2 OCSP extensions..... 38
- 8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS 39**
 - 8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT 39
 - 8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR 39
 - 8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY 39
 - 8.4 TOPICS COVERED BY ASSESSMENT..... 39
 - 8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY 39
 - 8.6 COMMUNICATION OF RESULTS..... 40
- 9 OTHER BUSINESS AND LEGAL MATTERS..... 41**
 - 9.1 FEES 41
 - 9.1.1 Certificate issuance or renewal fees..... 41
 - 9.1.2 Certificate access fees..... 41
 - 9.1.3 Revocation or status information access fees 41
 - 9.1.4 Fees for other services 41
 - 9.1.5 Refund policy 41
 - 9.2 FINANCIAL RESPONSIBILITY 41
 - 9.2.1 Insurance coverage 41
 - 9.2.2 Other assets..... 41
 - 9.2.3 Insurance or warranty coverage for end-entities 41
 - 9.3 CONFIDENTIALITY OF BUSINESS INFORMATION..... 42
 - 9.3.1 Scope of confidential information..... 42
 - 9.3.2 Information not within the scope of confidential information..... 42
 - 9.3.3 Responsibility to protect confidential information 43
 - 9.4 PRIVACY OF PERSONAL INFORMATION..... 43
 - 9.4.1 Privacy plan 43
 - 9.4.2 Information treated as private 43
 - 9.4.3 Information not deemed private 43
 - 9.4.4 Responsibility to protect private information..... 43
 - 9.4.5 Notice and consent to use private information 43
 - 9.4.6 Disclosure pursuant to judicial or administrative process..... 43
 - 9.4.7 Other information disclosure circumstances..... 43
 - 9.5 INTELLECTUAL PROPERTY RIGHTS 44
 - 9.6 REPRESENTATIONS AND WARRANTIES 44
 - 9.6.1 CA representations and warranties 44
 - 9.6.2 RA representations and warranties 44
 - 9.6.3 Subscriber representations and warranties 45
 - 9.6.4 Relying party representations and warranties 45
 - 9.6.5 Representations and warranties of other participants 45
 - 9.7 DISCLAIMERS OF WARRANTIES 45
 - 9.8 LIMITATIONS OF LIABILITY 46
 - 9.9 INDEMNITIES..... 47
 - 9.10 TERM AND TERMINATION 47
 - 9.10.1 Term..... 47
 - 9.10.2 Termination 47
 - 9.10.3 Effect of termination and survival..... 47
 - 9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS..... 47
 - 9.12 AMENDMENTS..... 47
 - 9.12.1 Procedure for amendment 48
 - 9.12.2 Notification mechanism and period..... 48
 - 9.12.3 Circumstances under which OID must be changed 48
 - 9.13 DISPUTE RESOLUTION PROVISIONS 48
 - 9.14 GOVERNING LAW 48

9.15 COMPLIANCE WITH APPLICABLE LAW 48

9.16 MISCELLANEOUS PROVISIONS..... 49

 9.16.1 Entire agreement 49

 9.16.2 Assignment 50

 9.16.3 Severability 50

 9.16.4 Enforcement (attorneys' fees and waiver of rights) 50

 9.16.5 Force Majeure 50

9.17 OTHER PROVISIONS 50

ACRONYMS..... 51

GLOSSARY..... 52

CERTIFICATE POLICY SUMMARY

Overview

This document defines the Certificate Policy (CP) for the RSA[®] ROOT SIGNING SERVICE in creating keys for signing, and signing and issuing certificates and keys to customers. Sections that have a heading "Signature" contain information pertaining only to a digital signing policy. A digital signing policy is designed to define the rules for signing certificates, documents and objects with a private key. Sections that have a heading "Confidential" pertain only to a confidential policy. Confidential policy describes the use of a private encryption key for protecting information and documents. All other sections apply to both Signature and Confidentiality. This policy governs the RSA ROOT SIGNING SERVICE and their customers. The CP sets forth the business, legal and technical requirements for approving, managing, revoking, and renewing digital certificates within the RSA ROOT SIGNING SERVICE.

This document is intended for users of the RSA ROOT SIGNING SERVICE and customer organizations that are interested in chaining their Certificate Authority hierarchy to the public key of the RSA ROOT SIGNING SERVICE root.

The RSA ROOT SIGNING SERVICE CP generally conforms both to the IETF PKIX Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practice Statement Framework (also known as RFC 3647). This document is divided into eight sections:

- Section 1 - Provides an overview of the policy and set of provisions, as well as the types of entities and the appropriate applications for certificates.
- Section 2 - Contains any applicable provisions regarding identification of the entity or entities that operate repositories; responsibility of a PKI participant to publish information regarding its practices, certificates, and the current status; frequency of publication; and access control on published information.
- Section 3 - Covers the identification and authentication requirements for certificate related activity.
- Section 4 - Deals with certificate life-cycle management and operational requirements including application for a certificate, revocation, suspension, audit, archival and compromise.
- Section 5 - Covers facility, management and operational controls (physical and procedural security requirements).
- Section 6 - Provides the technical controls with regard to cryptographic key requirements.
- Section 7 - Defines requirements for certificate, Certificate Revocation List (CRL) and Online Certificate Status Protocol (OCSP) formats. This includes information on profiles, versions, and extensions used.
- Section 8 - Addresses topics covered and methodology used for assessments/audits; frequency of compliance audits or assessments; identity and/or qualifications of the personnel performing the audit or assessment; actions taken as a result of deficiencies found during the assessment; and who is entitled to see results of an assessment.
- Section 9 - Covers general business and legal matters: the business issues of fees, liabilities, obligations, legal requirements, governing laws, processes, and confidentiality.

The RSA Root Signing Root CA's operate in an offline mode. The following Root CA certificates have been submitted to Application vendors for incorporation into their trusted Root store;

- the RSA Root CA (1024v1, known as the - Valicert Class 3 CA),

- the RSA Public Root CA v2
- the RSA Security 2048 v3

Additionally, the RSA Public Root CA v1 has been implemented as an intermediate X.509 version 3 CA to the RSA Root CA and is used to sign Participating CAs. This allows the RSA ROOT SIGNING SERVICE to provide version 3 functionality to Participating CAs through the RSA Root CA. The RSA Public Root CA v2 has been implemented to sign participating CAs and also has a trust relationship established with the RSA Root CA to provide ubiquity to users of earlier application releases. The RSA Security 2048 v3 has been implemented and will also be used to sign Participating CAs. As additional features and functionality are required by the industry and RSA customers, additional Root Certificate Authorities maybe be created.

The RSA ROOT SIGNING SERVICE Root CAs are also referred to as the "**RSA PUBLIC ROOT CA's**" throughout this document. A customer CA will be chained to the RSA ROOT SIGNING SERVICE root. The term "**participating CA**" refer to CAs that are chained to the RSA ROOT SIGNING SERVICE root. When the term "**CA**" or "**CAs**" is used, it implies all CAs within the RSA ROOT SIGNING SERVICE.

Introduction

RSA helps organizations build secure, trusted foundations for e-business through its RSA SecurID® two-factor authentication, RSA BSAFE® encryption, RSA ClearTrust access management and RSA digital certificate management systems. With approximately one billion RSA BSAFE-enabled applications in use worldwide, more than fifteen million RSA SecurID authentication users and over 20 years of industry experience, RSA has the proven leadership and innovative technology to address the changing security needs of e-business and bring trust to the online economy. Backed by the research of RSA Laboratories, RSA continues to develop innovative products and services that help secure enterprises and applications for hundreds of millions of users worldwide.

Since its introduction in 1999, the RSA certificate management solution has quickly become a market leader in public-key infrastructure (PKI) products and services. RSA is leveraging its leadership position in PKI with a natural extension of the RSA certificate management solution: the **RSA ROOT SIGNING SERVICE**. Based on proven, scaleable RSA certificate management technology, the **RSA ROOT SIGNING SERVICE** is designed to provide organizations who want to deploy PKI-enabled applications with even higher levels of flexibility and choice. Customers can now enable their secure e-business applications by deploying RSA Certificate Management software through a traditional in-house product implementation.

The RSA ROOT SIGNING SERVICE leverages the technical expertise of RSA Professional Services during the setup and implementation phase, as well as for integration and automation of customer-specific certificate enrollment/approval processes based on the RSA OneStep product. This capability is designed to provide the RSA ROOT SIGNING SERVICE customers with tremendous flexibility, while allowing them to maintain ultimate control over their security policies and certificate lifecycle management. And of course, the RSA ROOT SIGNING SERVICE includes ongoing access to high-quality, responsive technical support from the RSA Customer Support organization.

RSA with this certificate policy document and the accompanying CPS addresses the requirements as set forth by the CA/Browser Forum Guidelines for Extended Validation Certificates (<http://www.cabforum.org>). RSA complies with the version of the EV Certificate Guidelines adopted by the WebTrust Certification Authorities Advisory Group as the basis for WebTrust EV audit criteria. The Guidelines describe in detail what a CA must do in order to issue EV SSL certificates. Information about the issuing organization is displayed in a compatible browser that provides the end user a trustworthy confirmation of the identity of the entity that controls the website they are accessing.

POLICY SPECIFICATION

1 INTRODUCTION

1.1 Overview

This CP describes the assurance that may be placed on a certificate issued by a participating CA chained to the RSA Public Root CAs. Specifically, this CP defines the legal, business and technical requirements for the RSA ROOT SIGNING SERVICE in conjunction with its CPS and applicable agreements. The RSA Public Root CAs will issue certificates to CAs chaining them to one of the RSA Public Root CAs. These CAs are referred to as participating CAs. These participating CAs may issue certificates and sign keys for sub-CAs, Subscribers, devices, applications and other end entities.

1.2 Document name and identification

This CP is titled RSA Root Signing Service Certificate Policy or "**RSA RSS CP**".

The object identifier (OID) used for certificates (except for EV certificates) issued under this CP is: 1.2.840.113549.5.6.1; the OID for EV certificates issued under this CP is [1.2.840.113549.5.6.2](#).

1.3 PKI participants

The community governed by this CP are participating CAs hosted by the RSA ROOT SIGNING SERVICE, in particular the participating CAs that are chained to the RSA ROOT SIGNING SERVICE root. Under this CP, they will only issue CA certificates. End entity certificates may be issued, but only as required to administer the CA under this CP.

All participating CAs are obligated to issue, recognize and support all policies as stipulated here in this Certificate Policy that are relevant and in accordance to their business requirements. A CA may also issue, recognize and support additional Certificate Policies.

1.3.1 Certification Authorities (CA)

The RSA PUBLIC ROOT CA V1 is responsible for issuing certificates to participating CAs. These certificates bind the name of a participating CA to the public key needed to validate signatures generated by that participating CA.

All participating CAs operating under the RSA Public Root CAs are responsible for the following.

SIGNATURE

- Creating and signing of certificates binding Subscribers, PKI personnel and as required sub-CAs with their signature verification keys
- Promulgating certificate status through CRLs and/or OCSP responders, and
- Requiring adherence to this certificate policy

CONFIDENTIAL

- Creating, storing and recovering end entity confidential key pairs if required
- Promulgating certificate status through CRLs and/or OCSP responders, and
- Creating and signing of certificates binding Subscribers, and PKI personnel with their public encryption key

1.3.2 Registration Authorities (RA)

An RA Administrator or Vettor operating under this CP is responsible for all duties assigned to it by the issuing CA.

An RA Administrator or Vettor may perform duties on behalf of more than one CA, providing that in doing so it satisfies all requirements of this CP and it is not otherwise contractually prohibited from doing so.

1.3.3 Subscribers

Individuals and/or organizations may be Subscribers. In the case of the RSA Public Root CAs, the Subscriber is a CA chained to the root. Participating CAs chained to the RSA Public Root CAs may issue certificates for assignment to devices, groups, organizational roles, applications or end users. Responsibility and accountability for each certificate shall be attributable to an identified individual.

Eligibility for a certificate is at the sole discretion of the issuing CA.

A CA may administer any number of Subscribers.

1.3.4 Relying parties

A Relying Party may be either a Subscriber of any RSA Public Root CAs or any other person, application or device that is relying on a certificate issued by a CA that is chained to the RSA Public Root CAs root.

1.3.5 Other participants

No stipulation.

1.4 Certificate usage

This CP is applicable to all certificates issued and distributed by participating CAs. The policies described in this CP apply to the issuance, utilization and revocation of certificates within the RSA ROOT SIGNING SERVICE.

1.4.1 Appropriate certificate uses

Certificates issued under this CP by participating CAs that are chained to the RSA ROOT SIGNING SERVICE root are suitable for:

SIGNATURE

This policy is designed to be suitable for protecting the integrity and authenticity of business transactions as well as providing non-repudiation.

CONFIDENTIAL

This policy is designed to be suitable for certificate use such as encryption of information to facilitate the confidential transfer of that information.

1.4.2 Prohibited certificate uses

Certificates issued under this CP by participating CAs that are chained to the RSA ROOT SIGNING SERVICE root are prohibited under any other use not specified in Section 1.4.1.

In the case that participating CAs that are chained to the RSA ROOT SIGNING SERVICE will issue EV SSL certificates, the issuing CA must not issue EV Certificates to any person or any organization or entity that does not satisfy the requirements of the EV Certificate Guidelines.

1.5 Policy administration

RSA Security Policy Management Authority is the overall administrative authority of this CP.

1.5.1 Organization administering the document

RSA Security Policy Management Authority is the responsible authority for reviewing and approving changes to the RSA RSS CP. Written and signed comments on proposed changes shall be directed to the RSA Security contact as described in Section 1.5.2. Decisions with respect to the proposed changes are at the sole discretion of the RSA Security Policy Management Authority.

1.5.2 Contact person

The following is the primary contact for the RSA ROOT SIGNING SERVICE:

RSA ROOT SIGNING SERVICE Manager

RSA, The Security Division of EMC

174 Middlesex Turnpike

Bedford, MA 01730

781-515-5000

rsarootsign@rsa.com

General inquires may be sent to:

rsarootsign@rsa.com

1.5.3 Person determining CPS suitability for the policy

RSA ROOT SIGNING SERVICE is the administrative entity for determining Certification Practice Statement (CPS) suitability to this CP.

1.5.4 CPS approval procedures

The RSA ROOT SIGNING SERVICE will review any modifications, additions or deletions from all CPSs that are obligated to be compliant with this CP, and determine if modifications, additions or deletions are acceptable and do not jeopardize operations or the security of the CA environment.

1.6 Definitions and acronyms

A list of definitions and acronyms can be found at the end of this document.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

A Participating CA shall have at least one certificate repository (e.g. CA database, LDAP directory) and one CRL repository associated with the CA. A repository may or may not be on the same hosting system as the CA, and either certificates or CRLs may be published to a remote repository such as a standards-based LDAP directory. CRLs may be published to a web site to facilitate accessibility. Where the certificate and CRL repository is operated in a different computing environment other than the Participating CA, the certificate and CRL content shall remain under control of the CA.

The CA:

1. Shall make available, to Relying Parties, certificate revocation information (CRLs or OCSP (Online Certificate Status Protocol) server) published by the CA in accordance with the requirements of Sections 4.9 and 4.10
2. Include within any certificate it issues the URL of the website maintained by, or on behalf of, that CA
3. Should make available a copy of this CP and the CA's CPS for subscriber and relying party review
4. Publish its CP on a web site maintained by, or on behalf of that CA, the location of which shall be indicated in compliance with Section 9
5. Provide full text version of the CPS when necessary for the purposes of audit, accreditation or cross certification or as required by law.

The CA issuing EV certificates must maintain a repository that is available 24/7 whereby clients of the issuing CA can check online the status of all certificates.

2.2 Publication of certification information

Subscribers shall be notified that a CA may publish information submitted by them to publicly accessible directories in association with certificate status information. The publication of this information will be within the limits of sections 9.3 and 9.4.

CRL publication shall be in accordance with Section 4. A CA will publish certificate status information in frequent intervals as indicated in its CPS.

A Participating CA may retain an online repository of documents where it makes certain disclosure about its practices, procedures and the content of certain of its policies including its CPS and this CP. A Participating CA reserves has the right to make available and publish information on its policies by any means it sees fit. Due to their sensitivity, a Participating CA may refrain from making publicly available certain subcomponents and elements of such documents including, but not limited to, certain security controls and procedures related to the CA functioning.

2.3 Time or frequency of publication

Certificates information shall be distributed and/or published promptly upon issuance. Maximum time limits and frequency will be described in the Participating CA CPS.

2.4 Access controls on repositories

A Participating CA shall keep access to its public repository available to Relying Parties with the purpose of validating issued certificates. A Participating CA may limit or restrict access to its services such as the publication of status information on third party databases, and private directories.

Access controls may be instituted, at the discretion of a Participating CA, with respect to certificate status. A CA shall use commercially reasonable efforts to provide Relying Parties unrestricted access, either directly or by agreement, to the CRLs.

A Participating CA shall require, directly or through agreement with a repository, that operating and repository access controls will be configured so that only authorized CA personnel can write or modify the online version of the CP.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

Each entity shall have a clearly distinguishable and unique X.501 Distinguished Name (DN) in the certificate subject name field in accordance with PKIX Part 1. Each entity may use an alternative name via the SubjectAlternateName field, which also shall be in accordance with PKIX Part 1. The DN shall be in the form of a X.501 printableString or UTF8String and shall not be blank.

For Subordinate CAs not controlled by the same entity as the Root CA that will issue EV certificates the certificate's Subject field should conform to PKIX standard with an ASN.1 OID of 2.5.4.10, the field must be the full legal incorporated name. In addition an assumed name or d/b/a name may be used in the Subject field provided the full legal name follows in parenthesis. In such cases the string of characters cannot exceed 64 bytes, as defined by RFC 3280; otherwise only the full legal name shall be used.

3.1.2 Need for names to be meaningful

The contents of each certificate Subject and Issuer name field shall have an association with the authenticated name of the entity. The Relative Distinguished Name (RDN) should reflect the authenticated legal name of the entity.

In cases regarding the issuance of EV certificates, Distinguished Names will be the full legal name used for incorporation, or an assumed name or d/b/a (doing-business-as).

3.1.3 Anonymity or pseudonymity of subscribers

In exceptional cases where the identity of the Subscriber is protected; the name could be a combination of alphanumeric characters.

3.1.4 Rules for interpreting various name forms

No stipulation.

3.1.5 Uniqueness of names

Distinguished names shall be unique for all end entities of each participating CA. If applicable, for each end entity where the RDN is similar, additional number or letters may be appended to provide the RDN's uniqueness. The unique identifiers capability to differentiate Subscribers with identical names will not be supported.

For participating CAs that will issue EV SSL certificates, Distinguished Names (DNs) will be unique within their domain, and will not be ambiguous.

3.1.6 Recognition, authentication, and role of trademarks

The priority to entity names will be given to registered trademark holders.

The use of a Domain Name is restricted to the authenticated legal owner of that Domain Name.

The use of an email address is restricted to the authenticated legal owner of that email address.

A participating CA reserves the right to resolve all disputes regarding entity names in all assigned certificates. A party requesting a certificate shall demonstrate its right to use a particular name.

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

The method to prove possession of a private key shall be PKCS #10, or another cryptographically equivalent request (digitally signed request with private key).

3.2.2 Authentication of organization identity

An application for an organization to become a Subscriber shall be made by a person authorized to act on behalf of the organization. The details of this application shall conform to the requirements as set forth in the issuing CA's CPS and include details about the organization and include a certified true copy of their incorporation papers.

Identification and authentication of an applicant shall follow Section 3.2.3 as if that individual was applying for the certificate on its own behalf.

A CA shall verify the identity and employment status of the individual making the application and their authority to receive the keys for that organization.

A CA shall keep a record of the type and details of the identification used for the authentication of the organization for at least the life of the issued certificate.

3.2.3 Authentication of individual identity

An application for an individual to be a Subscriber may be made by the individual, or by another person or organization legally authorized to act on behalf of the prospective Subscriber. Background checks will be performed by the organization responsible for the issuing CA. A CA shall keep a record of the type and details of identification used for the authentication of the individual for at least the life of the issued certificate.

Identification and authentication of a prospective Subscriber shall be through one of the following means:

1. In person where the Certification Authority will compare the identity of the individual with a picture identification (notarized copies or originals), or
2. On line where the Subscriber agrees to the terms and conditions of an online Subscriber Agreement, the Subscriber completes an online form and the CA performs an out-of-band validation check on the information submitted, or
3. If the Certification Authority has previously established the identity of an individual using a process that satisfies the RSA ROOT SIGNING SERVICE management, and there has been no change in information presented, the Certification Authority may utilize privately shared information (referred to as a shared secret).
4. In cases where the individual subscriber will issue EV SSL certificates, validation of the said individual will conform to the CA's CPS. The vetting process must be based on the CA/Browser Guidelines concerning validation of an individual's identity.

3.2.4 Non-verified subscriber information

A Participating CA will identify in its CPS the submitted Subscriber information that is not verified as part of a certificate request.

3.2.5 Validation of authority

An application for a certificate shall be made by an individual or independent source that is accountable and responsible for the entity participating in the service. A CA or RA, on behalf of a CA, shall validate that the following have been verified in accordance with their CPS:

1. The identity of the individual making the application
2. The validity of that organization's business relationship with the CA, and
3. The authority of the individual to receive the certificate(s) for that organization application service

3.2.6 Criteria for interoperation

A CA will identify all procedures and requirements with respect to an application for a cross certificate in its Cross Certification Procedures. An application for cross certification does not oblige a CA to issue a cross certificate. A CA that is applying for cross certification shall provide with each application:

1. Its Certificate Policy
2. An external audit report validating compliance of the CA to its CP and CPS
3. The public verification key generated by the CA. and
4. A public verification key generated by the individual responsible for and authorized to act on behalf of the CA

Prior to submitting an application for a cross certificate a separate agreement which details the assurance levels and the other terms of the arrangement must be entered into between the cross certifying CAs, and the RSA Public Root CAs.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

Prior to the expiry of a private key, a request for a re-key may only be made by the entity in whose name the keys have been issued. An issuing CA shall authenticate all requests for re-key, and the subsequent response shall be authenticated by the entity. An entity requesting re-key may authenticate the request for re-key using a digital signature generated with the private key corresponding to the certified public key. Where the digital signature private key has expired, the request for re-key shall be authenticated in the same manner as the initial registration. In the case where there is a shared secret, the issuing CA may re-authenticate the Subscriber using the shared secret.

In all cases re-key requires the replacement of the public key in the certificate. A new public/private key pair is generated and a new certificate is issued.

3.3.2 Identification and authentication for re-key after revocation

Where the information contained in a certificate has changed or there is a known or suspected compromise of the private key resulting in a revocation, the CA or RA shall authenticate a re-issuance in the same manner as for initial registration pursuant to Section 3.2. An issuing CA shall verify any change in the information contained in a certificate before that certificate is issued.

3.4 Identification and authentication for revocation request

A Certification Authority shall authenticate a request for revocation of a certificate. A Certification Authority shall establish the process by which it addresses such requests and the means by which it will establish the validity of the request. A Certification Authority shall keep a record of the type and details of the revocation request including the identity and authentication of the requesting person.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

A CA shall require that all procedures and requirements with respect to an application for a certificate be set out in their CPS or a publicly available document. Bulk applications on behalf of end entities are permitted to be made only by persons authorized to make such applications. An application for a certificate does not oblige a CA to issue a certificate.

An application for a certificate does not oblige a CA to issue a certificate.

4.1.1 Who can submit a certificate application

An organization that has agreed to and executed an RSA Root Signing Agreement, and meets the requirements of the RSA ROOT SIGNING SERVICE can submit a certificate application as a Participating CA.

A Participating CA shall require that all Subscribers be an entity or agent with a valid contract with the organization participating in the RSA ROOT SIGNING SERVICE that has a valid business relationship with that organization and be bound to comply with provisions of such business relationship and any applicable agreement or corporate policies.

Any Subscriber information shall be complete, validated and accurate with full disclosure of all required information in connection with a certificate request.

A CA will identify all procedures and requirements with respect to an application for a cross certificate in its Cross Certification Procedures. An application for cross certification does not oblige a CA to issue a cross certificate. A CA that is applying for cross certification shall provide with each application:

1. Its Certificate Policy
2. An external audit report validating compliance of the CA to its CP and CPS
3. The public verification key generated by the CA, and
4. A public verification key generated by the individual responsible for and authorized to act on behalf of the CA.

If the CA will issue EV SSL certificates, its CPS must adhere to the Guidelines for EV Certificates by the CA/Browser Forum.

4.1.2 Enrollment process and responsibilities

Subscribers registering for a certificate from a CA will be required to consent to a Subscriber Agreement or equivalent agreement, either at the time of registration or upon certificate acceptance.

Prior to submitting an application for a cross certificate a separate agreement which details the assurance levels and the other terms of the arrangement must be entered into between the cross certifying CAs and the RSA Public Root CAs.

4.2 Certificate application processing

A CA shall require that each application be accompanied by:

1. Proof of end entity identity
2. Proof of authorization for any requested certificate attributes

3. A signed agreement of the applicable terms and conditions governing the applicants use of the certificate (may be a paper agreement or an "I accept" button), and
4. A public verification key generated by the end entity

For applications by a subscriber who will issue EV SSL certificates, the CA shall require full validation of that subscriber entity or a legally authorized representative of the subscriber that vets all the required information from the subscriber per the CA's CPS and in conformance with the Guidelines for EV Certificates by the CA/Browser Forum.

4.2.1 Performing identification and authentication functions

A CA or, associated RA on behalf of the CA, shall perform identification and authentication procedures to validate a certificate application.

The process of validation of the applicant who will issue EV SSL Certificates will require of the applicant, the EV Certificate Request, a Subscriber Agreement and any additional documentation required to satisfy the requirements for approval of the certificate application.

4.2.2 Approval or rejection of certificate applications

A CA shall notify a Subscriber, directly or through the associated RA, that the CA has rejected or has accepted the certificate application, created a certificate, and provided the Subscriber with access to the certificate. The CA may provide access to the certificate through manual or automated processes.

CAs processing application requests for EV SSL certificates must record in detail every action taken to process the EV certificate application request. This applies to all registration agents (RAs) and subcontractors as well.

4.2.3 Time to process certificate applications

Processing time of a certificate application will be described in a CA's CPS.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

CAs issue certificates based on requests that are correctly and properly verified according to Section 3.1. The issuance, and delivery or publication of a certificate by a CA indicates a complete and final approval of the certificate application by the issuing CA.

CAs may NOT issue EV certificates without the applicant's agreement to a legally enforceable Subscriber Agreement.

4.3.2 Notification to subscriber by the CA of issuance of certificate

An issuing CA shall notify a Subscriber that the CA has created a Certificate, and provide the Subscriber with access to the Certificate by notifying them that their Certificate is available and notifying the Subscriber of the means for obtaining the Certificate.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

Notification by an issuing CA to a Subscriber of the publishing of the Subscriber's certificate in a repository or confirmation of delivery of Subscriber's certificate shall indicate approval of the

certificate and acceptance by both the CA and the Subscriber of the certificate. By accepting and using the certificate the Subscriber agrees to comply with the terms of any policies referenced within the certificate.

By accepting an EV certificate, the Subscriber:

1. Agrees to be bound by the continuing responsibilities, obligations and duties imposed by the issuing CA's CPS
2. Agrees to be bound by the Subscribing Party agreement, and
3. Represents and warrants that to its knowledge no unauthorized person has had access to the private key associated with the certificate, and
4. Represents and warrants that the certificate information it has supplied during the registration process is truthful and has been accurately and fully published within the certificate.

4.4.2 Publication of the certificate by the CA

A CA is responsible for repository and publication functions. A CA shall publish certificates in a repository based on the certificate publishing practices of the issuing CA (as defined in the CPS), as well as revocation information concerning such certificates.

4.4.3 Notification of certificate issuance by the CA to other entities

No stipulation.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

The Subscriber shall only use certificates, issued under the RSA ROOT SIGNING SERVICE, and their associated key pairs for the purposes identified in this CP, the agreed upon RSA Root Signing Agreement and any applicable Subscriber Agreement.

4.5.2 Relying party public key and certificate usage

Prior to using a Subscriber's certificate, a Relying Party should verify that the certificate is appropriate for the intended use.

4.6 Certificate renewal

4.6.1 Circumstance for certificate renewal

Certificate renewal is the re-issuance of a certificate with a new validity date using the same public key corresponding to the same private key. Certificate renewal will only be permitted within a time range prior to certificate expiration, as defined in the CA's CPS and the agreed upon RSA Root Signing Agreement.

4.6.2 Who may request renewal

An organization that has a valid RSA Root Signing Agreement, and meets the requirements of the RSA ROOT SIGNING SERVICE can submit a certificate to be renewed.

A Participating CA shall require that a Subscriber is currently in possession of a valid certificate and remains an entity or agent of the organization participating in the RSA ROOT SIGNING SERVICE. The Subscriber must have a valid business relationship with that organization and be bound to comply with provisions of such business relationship and any applicable agreement or corporate policies.

4.6.3 Processing certificate renewal requests

Subscribers requesting certificate renewal must be in possession of a valid certificate and be directed to a renewal server. The Subscriber shall be tightly bound to their public keys and the information submitted.

CAs processing renewal requests for EV SSL certificates must record in detail every action taken to process the EV certificate renewal request. This applies to all registration agents (RAs) and subcontractors as well.

4.6.4 Notification of new certificate issuance to subscriber

A Subscriber will be notified by an issuing CA of the publishing of the Subscriber's certificate in a repository or confirmation of the delivery of Subscriber's certificate.

4.6.5 Conduct constituting acceptance of a renewal certificate

Notification by an issuing CA to a Subscriber of the publishing of the Subscriber's certificate in a repository or confirmation of delivery of Subscriber's certificate shall indicate approval of the certificate and acceptance by both the CA and the Subscriber of the certificate renewal. By accepting and using the certificate the Subscriber agrees to comply with the terms of any policies referenced within the certificate.

4.6.6 Publication of the renewal certificate by the CA

A CA is responsible for repository and publication functions. A CA shall publish renewed certificates, as per the initial enrollment, in a repository based on the certificate publishing practices of the issuing CA (as defined in the CPS), as well as revocation information concerning such certificates.

4.6.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.7 Certificate re-key

4.7.1 Circumstance for certificate re-key

Routine re-key is not supported. Prior to the expiry of a public/private key pair, an authorized individual representing the particular public/private key pair that is about to expire will be required to make a new certificate request.

An RA, on behalf of the issuing CA, shall authenticate all requests in the same manner as the initial application.

4.7.2 Who may request certification of a new public key

No stipulation.

4.7.3 Processing certificate re-keying requests

No stipulation.

4.7.4 Notification of new certificate issuance to subscriber

No stipulation.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

No stipulation.

4.7.6 Publication of the re-keyed certificate by the CA

No stipulation.

4.7.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.8 Certificate modification

4.8.1 Circumstance for certificate modification

A certificate may be modified:

1. At the CA's discretion, when the basis for any information in the certificate changes.
2. A change in the business relationship or status* under which the certificate was issued occurs.

* If the company or individual are elevated to high-risk status.

The issuing CA must revoke a certificate if the issuing CA suspects that the modifications to the certificate potentially compromise a Subscriber's keys or certificates.

4.8.2 Who may request certificate modification

The issuing CA's CPS will identify who can request for a certificate to be modified.

4.8.3 Processing certificate modification requests

The procedures and requirements with respect to the modification of a certificate are set out in the respective CA CPS.

For modifications to EV certificates; in such cases the new information gathered will need to undergo the same validation process that was employed during the initial application with the CA.

4.8.4 Notification of new certificate issuance to subscriber

Notification by an issuing CA to a Subscriber of the publishing of the Subscriber's modified certificate in a repository or confirmation of delivery of Subscriber's certificate by the Subscriber shall indicate notification of issuance of the certificate.

4.8.5 Conduct constituting acceptance of modified certificate

Notification by an issuing CA to a Subscriber of the publishing of the Subscriber's certificate in a repository or confirmation of delivery of Subscriber's certificate by the Subscriber shall indicate acceptance by both the CA and the Subscriber of the modified certificate. By accepting and using the certificate the Subscriber agrees to comply with the terms of any policies referenced within the certificate.

4.8.6 Publication of the modified certificate by the CA

A CA is responsible for repository and publication functions. A CA shall publish modified certificates, as per the initial enrollment, in a repository based on the certificate publishing practices of the issuing CA (as defined in the CPS), as well as revocation information concerning such certificates.

4.8.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

A certificate should be revoked:

1. When any information in the certificate changes
2. Upon suspected or known compromise of the private key
3. Upon suspected or known compromise of the media holding the private key
4. Upon termination of a Subscriber, or
5. When a Subscriber no longer needs access to secured organizational resources

A Certification Authority in its discretion may revoke a certificate when an entity fails to comply with obligations set out in this CP, its CPS, any applicable agreement or applicable law. The issuing CA may revoke a certificate at any time if the issuing CA suspects that conditions may lead to a compromise of a Subscriber's keys or certificates.

When a CA is cross certified with a participating CA, either CA may revoke the cross certificate:

1. when any of the information in the cross certificate changes
2. Upon suspected or known compromise of a CA's private key
3. Upon suspected or known compromise of media holding a CA's private key

4. When a CA fails to comply with obligations set out in its CP, any applicable agreement or any applicable law.
5. For revocation requests for EV SSL certificates:
 - A) In the specific instances where it becomes necessary for the CA to revoke EV certificates, the CA must publish those guidelines in its CPS.
 - B) The CA must publish clear guidelines for revoking EV Certificates as part of its EV Practices, and maintain a continuous 24/7 ability to accept and respond to revocation requests and related inquiries.

4.9.2 Who can request revocation

The revocation of a certificate may only be requested by:

1. The Subscriber whose name the certificate is issued under
2. The individual or organization which made the application for the certificate on behalf of an organization, device or application
3. Personnel of an RA associated with the issuing CA
4. Personnel of the issuing CA
5. Individuals that request the revocation of EV certificates must be authorized by the CA in adherence to the stipulations in its CPS and Subscriber Agreement

The revocation of a cross certificate may only be requested by:

1. A CA on whose behalf the cross certificate was issued, or
2. The personnel operating the CA

4.9.3 Procedure for revocation request

The procedures and requirements with respect to the revocation of a certificate are set out in the respective CA CPS.

All requests for revocation shall be submitted to the CA or RA, on behalf of the CA, via an approved online process or in writing. The authenticated revocation request and any resulting actions taken by the CA shall be recorded and retained as required. In the case when a certificate is revoked, justification for the revocation shall also be documented.

When a Subscriber certificate is revoked, the revocation shall be published in the appropriate CRL of the issuing CA.

4.9.4 Revocation request grace period

The request for revocation grace period shall be defined in the Service Level Agreement, contract or the associated CPS.

4.9.5 Time within which CA must process the revocation request

The time within a CA must process a revocation request shall be defined in the associated CA's CPS.

4.9.6 Revocation checking requirement for relying parties

Prior to using a certificate, it is the Relying Party's responsibility to check the status of all certificates in the certificate validation chain against the current CRLs or online certificate status

server. A Relying Party is also responsible for verifying the authenticity and integrity of CRLs or online certificate status response. The CA providing the certificate status information shall identify the access point to the CRL or online certificate status server in every certificate it issues as well as in its CPS.

4.9.7 CRL issuance frequency

A CA shall issue an up to date CRL, as required, to attest the most current certificate status of all issued certificates. A CA shall synchronize its CRL issuance with any directory synchronization to provide accessibility of the most recent CRL to Relying Parties. The CRL issuance frequency shall be defined in the associated CA's CPS.

4.9.8 Maximum latency for CRLs

A CA shall synchronize, automatically or manually, its CRL issuance with an accessible directory or web site to provide accessibility of the most recent CRL to Relying Parties. The maximum latency period shall be defined in the associated CA's CPS.

4.9.9 Online revocation/status checking availability

On line certificate revocation status checking may be supported via Online Certificate Status Protocol (OCSP) server. If an online certificate status server is implemented, the OCSP Responder will be available for a high percentage of each 24-hour period. The OCSP availability requirements will be specified in the CA's CPS.

4.9.10 Online revocation checking requirements

If OCSP is implemented, applications should support OCSP and the Internet Engineering Task Force (IETF) RFC 2560. All OCSP responses shall be digitally signed by the CA or a private key signed by the CA. A Relying Party should check the status of all certificates in the certificate validation chain against the OCSP Responder prior to their use. A Relying Party should also verify the authenticity and integrity of the OCSP Responder.

4.9.11 Other forms of revocation advertisements available

No stipulation.

4.9.12 Special requirements re-key compromise

No stipulation.

4.9.13 Circumstances for suspension

Participating CAs may support the suspension of certificates. Certificate suspension is at the discretion of the issuing CA.

4.9.14 Who can request suspension

A suspension of a certificate may only be requested by:

1. The Subscriber
2. The individual or representative of an organization which made the application for a certificate on behalf of an organization, device or application
3. A manager on behalf of a Subscriber
4. Personnel of an RA associated with the issuing CA, or

5. Personnel of the Certification Authority

4.9.15 Procedure for suspension request

A CA shall define all procedures and requirements with respect to the suspension of a certificate in its CPS. An authenticated suspension request and any resulting action taken by the issuing CA shall be recorded and retained as required. In the case where a certificate is suspended, justification for the suspension shall be documented.

4.9.16 Limits on suspension period

The maximum length of time for the suspension of a certificate is 60 days unless otherwise approved by management of the issuing CA.

4.10 Certificate status services

4.10.1 Operational characteristics

Operational characteristics will be specified in the CA's CPS.

4.10.2 Service availability

Requirements will be specified in the CA's CPS.

4.10.3 Optional features

No stipulation.

4.11 End of subscription

The end of a subscription as a result of no longer requiring the service, compromise, or termination of employment (voluntary or imposed) will result in the immediate revocation of the certificate and the publishing of a CRL or other certificate status verification system.

4.12 Key escrow and recovery

4.12.1 Key escrow and recovery policy and practices

CA Private Signing Key shall not be escrowed.

Subscriber's digital signature private keys shall not be escrowed.

Subscriber's encryption private keys may be escrowed.

4.12.2 Session key encapsulation and recovery policy and practices

No stipulation.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical controls

CA facilities shall provide adequate physical security controls that meet the business requirement of the CAs being hosted and the compliance requirements of the RSA ROOT SIGNING SERVICE. These requirements will be further defined in a CA's CPS. The physical security controls must limit access to authorized personnel only. Subscribers shall satisfy the security requirements as documented in the issuing CA's CPS.

5.1.1 Site location and construction

The following requirements and procedures are to be implemented regarding the CA physical facility:

The CA site must:

- Satisfy at least the requirements for a Security Zone
- Be manually or electronically monitored for unauthorized intrusion at all times
- Ensure unescorted access to the CA server is limited to those personnel identified on an access list
- Ensure personnel not on the access list are properly escorted and supervised
- Ensure a site access log is maintained and inspected periodically, and
- Ensure all removable media and paper containing sensitive plaintext information is stored in containers that are physically secure such as a locked filing cabinet or a locked safe

The access control systems must be inspected:

- Be inspected at least quarterly by qualified personnel
- The inspection documentation must be retained for at least a one-year period to support audit requirements

All access control and monitoring systems must be tied to a UPS. The UPS system must be inspected:

- Be inspected at least annually
- The inspection documentation must be retained for at least a one-year period.

When a PIN or password is recorded, it shall be stored in a security container accessible only to authorized personnel.

All RA sites should be located in areas that satisfy the controls required for a Reception Zone. RA workstations should be located in areas where access is restricted to authorized personnel and where visitors are escorted. The RA host computer will be located in a secure space with appropriate physical security and access controls. The RA shall not leave the RA host computer unattended when the password or PIN that unlocks the RA certificate private signing key has been entered.

All media within or used by an RA administrator's workstation should be protected when the workstation is unattended.

A participating CA shall require that the operation of the RA site provide appropriate security protection of the cryptographic module, all system software and the RA Administrator's private key. All CAs shall conduct a threat and risk assessment of all RA operations. It is recommended that the RA Administrator:

1. secure private keys on a smart card token (smart card) based certificates, and require the token is secured when not in use
2. If RA private keys are stored in a password protected file on the computer hard drive, require boot-level access control and password protected screen saver

5.1.2 Physical access

As detailed in the CA's CPS.

5.1.3 Power and air conditioning

A CA must ensure that the power and air conditioning facilities are sufficient to support the operation of the CA system.

5.1.4 Water exposures

A CA must ensure that the CA system is protected from water exposure.

5.1.5 Fire prevention and protection

A CA must ensure that the CA system is protected from fire exposure with a fire suppression system.

5.1.6 Media storage

A CA must ensure that storage media used by the CA system is protected from environmental threats such as temperature, humidity and magnetism.

5.1.7 Waste disposal

A CA must ensure sanitization or destruction of all confidential media before release for disposal.

5.1.8 Off-site backup

A CA must ensure that facilities used for off-site backup have the equivalent level of security as the primary CA site.

5.2 Procedural controls

5.2.1 Trusted roles

A Certification Authority shall require a separation of duties for critical CA functions to prevent one person from maliciously using the CA system without detection. PKI Personnel access to the CA system(s) is to be limited to those actions for which they are required to perform in fulfilling their responsibilities.

A Certification Authority shall require that RA personnel understand their responsibility for the identification and authentication of prospective Subscribers and perform the following functions:

1. acceptance of applications, certificate changes, certificate revocation and key recovery requests
2. verification of an applicant's identity and authorizations
3. transmission of applicant information to the issuing CA, and
4. Provision of shared secrets, as required for authenticating Subscribers
5. For EV Certificate issuance, there should a validation specialist's role, or similar roles defined to handle the special requirements of vetting applicants. Any and all persons

associated with all phases of the EV certificate lifecycle shall be vetted and qualified to service any request or role in the lifecycle and shall be trained and audited to ensure compliance and quality assurance as measured by the issuing CA's CPS.

5.2.2 Number of persons required per task

A CA shall provide the proper security and procedures such that no single individual may perform CA activities. This practice is referred to as split knowledge and dual control¹.

Multi-user control is also required for CA key generation as outlined in Section 6.2.2.

A CA shall limit access such that no single individual may gain access to the Subscriber private keys stored by the issuing CA.

All other duties associated with CA roles may be performed by an individual operating alone. A CA shall require that any verification process it employs provides an oversight of all activities performed by privileged CA role holders.

5.2.3 Identification and authentication for each role

All CA personnel shall have their identity and authorization verified before they are:

1. Included in the access list for the CA site
2. Included in the access list for physical access to the CA system
3. Given a certificate for the performance of their CA role or
4. Given an account on the CA system

Each of these certificates and accounts (with the exception of the CA signing certificates) shall:

1. Be directly attributable to an individual
2. Not be shared, and
3. Be restricted to actions authorized for that role through the use of CA software, operating system and procedural controls

CA operations shall be secured, using commercially reasonable mechanisms such as token based strong authentication and encryption, when accessed across a shared network.

5.2.4 Roles requiring separation of duties

A CA shall require a separation of duties for critical CA functions to prevent one person from maliciously using the CA system without detection.

The CA must enforce rigorous control procedures for the separation of validation duties to ensure that no one person can single-handedly validate and authorize the issuance of an EV Certificate.

¹ As defined in ISO 9564-1, split knowledge is "a condition under which two or more parties separately and confidentially have custody of components of a single key that, individually, convey no knowledge of the resultant cryptographic key". The resultant key exists only within "secure cryptographic devices". Dual control is explained in the standard as "a process utilizing two or more separate entities (usually persons), operating in concert, to protect sensitive functions or information, whereby no single entity is able to access or utilize the materials, e.g., cryptographic key".

5.3 Personnel controls

A Certification Authority shall require that all personnel performing duties with respect to the operation of a CA shall:

1. Be appointed in writing
2. Be bound by contract or statute to the terms and conditions of the position they are to fill
3. Have received comprehensive training with respect to the duties they are to perform
4. Be bound by contract or statute not to disclose sensitive CA security-relevant information or Subscriber information, and
5. Not be assigned duties that may cause conflict with their CA duties

5.3.1 Qualifications, experience, and clearance requirements

A CA shall require that all personnel performing duties with respect to the operation of a CA have sufficient qualification and experience in PKI, All personnel shall meet organizational personnel security requirements.

5.3.2 Background check procedures

All background checks shall be performed in accordance with organizational policies and procedures of the issuing CA.

Prior to the commencement of employment of any person by the Participating CA for engagement in the EV Certificate process, whether as an employee, agent, or an independent contractor, of the CA, the CA must validate the eligibility of the person(s) through a process as defined by the issuing CA's CPS and in conformance with the CA/Browser Forum Guidelines for Extended Validation Certificates.

5.3.3 Training requirements

A CA shall provide comprehensive training for all personnel performing duties with respect to the operation of the CA.

5.3.4 Retraining frequency and requirements

The requirements for Section 5.3.3 shall be kept current to accommodate changes in a CA system. Refresher training shall be conducted as required, and management shall review these requirements once a year.

5.3.5 Job rotation frequency and sequence

No stipulation.

5.3.6 Sanctions for unauthorized actions

In the event of actual or suspected unauthorized action by a person performing duties with respect to the operation of a CA, that CA may suspend his or her access to the CA system. A Certification Authority may revoke a certificate when an entity fails to comply with obligations set out in this CP, its CPS, any applicable agreement or applicable law. A CA may revoke a certificate at any time if a CA suspects that conditions may lead to a compromise of keys or certificates.

5.3.7 Independent contractor requirements

A Certification Authority shall limit contractor access to the CA site in accordance with Section 5.3.

5.3.8 Documentation supplied to personnel

A CA should make its CA and RA personnel aware of the requirements of applicable Certificate Policies, Certification Practice Statements and any other specific policies, procedures, documents, and/or contracts relevant to their particular job requirements.

5.4 Audit logging procedures

5.4.1 Types of events recorded

A CA shall record in audit log files all relevant events relating to the security of that CA system. All relevant logs, whether electronic or manual, should contain the date and time of the event, and the identity of the entity which caused the event.

A CA shall indicate in their CPS what information is logged. All relevant agreements and correspondence should be collected and consolidated either electronically or manually in one single location to facilitate decision making.

The CA must record in detail every action taken to process an EV Certificate Request and to issue an EV Certificate, including all information generated or received in connection with an EV Certificate Request, and every action taken to process the Request, including time, date, and personnel involved in the action. These records must be available as auditable proof of the CA's Practices.

5.4.2 Frequency of processing log

The frequency of audit log reviews will be based on the security requirements of a CA. All significant events shall be explained in an audit log summary. Actions taken following these reviews shall be documented.

5.4.3 Retention period for audit log

A CA shall retain its audit logs for at least seven (7) years. A CA will retain audit logs in a manner described in Section 5.5.2.

5.4.4 Protection of audit log

The electronic audit log system shall include mechanisms to protect the log files from unauthorized viewing, modification or deletion.

Manual audit information shall be protected from unauthorized viewing, modification or deletion.

5.4.5 Audit log backup procedures

Audit logs and summaries of the inspection of audit logs shall be backed up or copied.

5.4.6 Audit collection system (internal vs. external)

A CA shall identify their audit collection systems in the CPS.

5.4.7 Notification to event-causing subject

When an event is logged by the audit collection system, no notice needs to be given to the individual or entity that caused the event.

5.4.8 Vulnerability assessments

Events in the audit process are logged, in part, to monitor system vulnerabilities. A CA shall perform a vulnerability assessment and action taken, as required, following an examination of these monitored events.

5.5 Records archival

5.5.1 Types of records archived

A CA shall indicate in their CPS what information is archived.

5.5.2 Retention period for archive

Digital Signature certificates, public verification keys, confidentiality private keys stored by the issuing CA, CRLs, and any other information generated by the issuing CA should be retained for a minimum of seven (7) years after the expiry of the key material. This requirement does not include the backup of private signature keys.

Audit information, Subscriber agreements and any identification and authentication information shall be retained for the length of time identified in the CA's CPS.

5.5.3 Protection of archive

Archived information shall include mechanisms to protect the log files from unauthorized viewing, modification or deletion.

Manually archived information shall be physically protected from unauthorized viewing, modification or deletion.

5.5.4 Archive backup procedures

Confidentiality private keys that are backed up by the issuing CA are to be protected at a level of physical and cryptographic protection equal to or exceeding that in place at the issuing CA site.

A second copy of all material retained or backed up should be stored in a location other than the issuing CA site and shall be protected either by physical security alone or a combination of physical and cryptographic protection. Any such secondary site shall provide adequate protection from environmental threats such as temperature, humidity and magnetism.

5.5.5 Requirements for time-stamping of records

All documents archived pursuant to this section shall be marked with the date of their creation or execution.

5.5.6 Archive collection system (internal or external)

No stipulation.

5.5.7 Procedures to obtain and verify archive information

A CA should verify the integrity of the backups at least once every 12 months to ensure usability of these backups. Material stored off-site shall be periodically verified for data integrity.

5.6 Key changeover

A Subscriber may only apply to renew his or her key pair within three (3) month prior to the expiration of the certificate providing that certificate has not been revoked or suspended. A Subscriber or the issuing CA may initiate this key changeover process. Automated key changeover is permitted. A CA shall require that the details of this key changeover process is indicated in its CPS.

Subscribers without valid keys shall be re-authenticated by the CA in the same manner as the initial registration. When a Subscriber's certificate has been revoked as a result of non-compliance, the issuing CA shall verify that reasons for non-compliance have been addressed to the issuing CA's satisfaction prior to certificate re-issuance. The subscriber will be required to generate a new public / private key pair when requesting certificate renewal if the certificate has been suspended or revoked.

Keys may not be renewed using expired Digital Signature keys.

5.7 Compromise and disaster recovery

A CA shall provide business continuity procedures in its CPS, Business Continuity Plan, or Disaster Recovery Plan that outline the steps to be taken in the event of corruption or loss of computing resources, software and/or data.

In the unlikely event that there is a compromise of a CA key, the CA shall notify its Subscribers promptly. Detailed instructions will be specified in the respective CA's CPS.

5.7.1 Incident and compromise handling procedures

Incident and compromise handling procedures will be provided in the CA Operations Procedures.

5.7.2 Computing resources, software, and/or data are corrupted

In the event of the corruption of computing resources, software, and/or data, such an occurrence is reported to the responsible DRP manager and incident handling procedures are to be enacted immediately. Such procedures require appropriate escalation, incident investigation, and incident response. If necessary, disaster recovery procedures will be enacted.

5.7.3 Entity private key compromise procedures

In the unlikely event that there is a compromise of a CA key with the Participating CA, all Subscribers will be notified promptly. Detailed instruction will be provided in the CA Operations Procedures.

Subscriber (end entity) key compromise will result in immediate revocation. Re-issuance will be in accordance with section 3.3.2.

5.7.4 Business continuity capabilities after a disaster

A CA shall provide business continuity procedures in a Disaster Recovery Plan that outline the steps to be taken in the event of corruption or loss of computing resources, software and/or data.

5.8 CA or RA termination

In the event that a CA ceases operation, it shall notify its Subscribers promptly upon termination of operations and all certificates and cross certificates should be revoked. The CA should arrange for the continued retention of the CA's keys and information. It shall also notify all CA's with whom it is cross certified. In the event of a change in management in a CA's operation, that CA should notify all entities for which it has issued certificates, CAs with whom it has cross certified and the RSA ROOT SIGNING SERVICE.

6 TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key pair generation

Each prospective certificate holder shall generate its own Digital Signature keys and may generate its own Confidentiality keys using an industry accepted algorithm.

6.1.2 Private Key delivery to subscriber

No stipulation.

6.1.3 Public key delivery to certificate issuer

All Subscriber public-keys and certificates will be stored in the CA's repository and/or LDAP directory. Delivery of Subscribers' public keys, from the Subscribers themselves or through an associated RA, shall be in PKCS #10 Certificate Signing Request (CSR) or equivalent format. When the CA or an RA generates Subscriber key pairs, this requirement is not applicable.

6.1.4 CA public key delivery to relying parties

The CA public key (as part of the certificate) shall be delivered to a Subscriber as part of the issuing process. The format must be DER encoded (binary or base64) or PKCS #7 (binary or base64), with or without chain, depending on the Subscribers' requirements and as outlined in the issuing CA's CPS.

6.1.5 Key sizes

A CA should require that the key pairs for all PKI entities be a minimum of 1024 bits in length and use the RSA algorithm for the key algorithm.

6.1.6 Public key parameters generation and quality checking

All CA Signature keys shall be generated using a random or pseudo-random process as described in ISO 9564-1 and ISO 11568-5 that are capable of satisfying the statistical tests of FIPS PUB 140-2, level 3. CA Keys are to be protected by a secure cryptographic hardware module rated at least FIPS 140-2, Level 3.

Subordinate CA shall generate signature keys using a random or pseudo-random process as described in ISO 9564-1 and ISO 11568-5 that are capable of satisfying the statistical tests of FIPS PUB 140-2, level 3. Subordinate CA Keys are to be protected by a secure cryptographic hardware module rated at least FIPS 140-2 level 3.

Key pairs for all other Subscribers may be generated and stored in software or protected by secure cryptographic hardware module (e.g. Smartcards) at the discretion of the issuing CA.

6.1.7 Key usage purposes (as per X.509 v3 key usage field)

Applicable agreements or contracts or statements of work shall govern key usage. In general:

SIGNATURE

Keys may be used for authentication, non-repudiation and message integrity. They may also be used for session key establishment.

CA signing keys are the only keys permitted to be used for signing certificates, CRLs and OCSP responses. Specific purpose keys may be generated by the CA for signing CRLs and OCSP responses.

CONFIDENTIAL

Keys may be used for exchange and establishment of keys used for session and data confidentiality.

The certificate KeyUsage field shall be used in accordance with PKIX-1 Certificate and CRL Profile.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

The certificate holder shall protect its private key from disclosure according to the requirements as defined by the issuing CA. The certificate holder is responsible for its private keys. Subscribers will change their passwords in accordance with the organization's security policy.

The private key of an entity shall be protected from unauthorized use by a combination of commercially reasonable cryptographic and physical access control mechanisms as defined by the issuing CA. The level of protection should be adequate to deter a motivated attacker with substantial resources. If a reusable password scheme is used, the mechanism should include a facility to temporarily lock the account after a predetermined number of login attempts.

6.2.1 Cryptographic module standards and controls

All CA Digital Signature key generation, CA Digital Signature key storage and certificate signing operations shall be performed in a hardware cryptographic module rated to at least FIPS 140-2 Level 3 or otherwise verified to an equivalent level of functionality and assurance. All other CA cryptographic operations, such as certificates and keys used for administering the CA, shall be performed in a cryptographic module validated to at least FIPS 140-2 Level 2 or otherwise verified to an equivalent level of functionality.

The RA Administrator Digital Signature key generation should be performed in a cryptographic module rated to at least FIPS 140-2 Level 1 or otherwise verified to an equivalent level of functionality and assurance.

End entities should use cryptographic modules validated to at least FIPS 140-2 Level 1 or otherwise verified to an equivalent level of functionality and assurance.

6.2.2 Private Key (n out of m) multi-person control

There shall be multiple person control for CA key generation operations. At a minimum, there shall be multi-person control for operational procedures such that no one person can gain control over the CA signing key. The principle of split knowledge and dual control as defined in section 5.2.2 shall be applied.

6.2.3 Private Key escrow

CA Private Signing Key should not be escrowed unless required. The storage of the CA Private Signing Key should have the same level of security as the primary site.

End Entity Private Keys:

SIGNATURE

Digital Signature private keys should not be escrowed.

CONFIDENTIAL

Private confidentiality keys may be escrowed.

6.2.4 Private Key backup

CA Private Signing Key will be backed up according to contractual requirements.

SIGNATURE

An entity may optionally back up its own Digital Signature private key. If so, the keys shall be copied and stored in encrypted form and protected at a level no lower than stipulated for the primary version of the key.

CONFIDENTIAL

Participating CAs may back up all private confidentiality keys that the CA issues.

6.2.5 Private Key archival

Refer to Section 5.5.

6.2.6 Private Key transfer into or from a cryptographic module

No stipulation.

6.2.7 Private Key storage on cryptographic module

CA digital signature key storage shall be kept on a secure cryptographic hardware module rated to at least FIPS 140-2 Level 3.

6.2.8 Method of activating private key

An entity must be authenticated to the cryptographic module before the activation of the private key. This authentication, at a minimum, will be in the form of a password. When deactivated, private keys must be kept in encrypted form only.

6.2.9 Method of deactivating private key

When keys are deactivated the application must clear the keys from memory before the memory is de-allocated. Any disk space where keys were stored must be over-written before the space is released to the operating system. The cryptographic module must automatically deactivate the private key after a pre-set period of inactivity defined in the CA's CPS.

6.2.10 Method of destroying private key

Upon termination of use of a private key, over-writing must securely destroy all copies of the private key in computer memory and shared disk space. Private Key destruction procedures must be described in the CPS.

6.2.11 Cryptographic Module Rating

All CA digital signature key generation, CA digital signature key storage and certificate signing operations shall be performed in a secure cryptographic hardware module rated to at least FIPS 140-2 Level 3 or otherwise verified to an equivalent level of functionality and assurance.

6.3 Other aspects of key pair management

6.3.1 Public key archival

The issuing CA shall retain all verification public keys for the period of time defined in its CPS.

6.3.2 Certificate operational periods and key pair usage periods

A participating CA private signing key will expire prior to the RSA Public Root CAs key that signed the participating CA private signing key.

Subscriber keys and certificates will expire prior to the issuing CA key that signed the Subscriber's public verification key. Key usage for 1024 bit keys should have a validity period that conforms to an organization's risk management model.

6.4 Activation data

6.4.1 Activation data generation and installation

If activation data is used it shall be unique and unpredictable.

6.4.2 Activation data protection

If activation data is used it, it shall be protected from unauthorized use by a combination of cryptographic and physical access control mechanisms.

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

The following functionality may be provided by the operating system, or through a combination of operating system, PKI CA software, and physical safeguards (policies and procedures). Each CA server should include the following functionality:

1. Access control to CA services and PKI roles
2. Enforced separation of duties for PKI roles
3. Identification and authentication of PKI roles and associated identities
4. Use of cryptography for session communication and database security
5. Archival of CA and end entity history, and audit data
6. Audit of security related events
7. Trusted path for identification of PKI roles and associated identities, and
8. Recovery mechanisms for keys and CA system

6.5.2 Computer security rating

No stipulation.

6.6 Life cycle technical controls

6.6.1 System development controls

All CAs should use CA software that has been designed and developed under a development methodology. The design and development process should be supported by a verification process to influence security safeguard design and minimize residual risk.

6.6.2 Security management controls

A formal configuration management methodology should be used for installation and ongoing maintenance of a CA system. CA software, when first loaded shall provide a method for a CA to verify that the software on the system is valid, The CA shall verify that the CA application:

- Originated from the software manufacture
- Has not been modified prior to installation, and
- Is the intended version

A CA shall provide a commercially reasonable mechanism to periodically verify the integrity of the software.

6.6.3 Life cycle security controls

No stipulation.

6.7 Network security controls

A CA shall use commercially reasonable efforts to protect its servers from attack through any open or general purpose network with which it is connected. Such protection shall be provided through a combination of hardware and/or software configured to allow only the protocols and commands required for the operation of the CA.

A CA shall define those protocols and commands required for the protection of the CA in its CPS or other procedural document.

6.8 Time-stamping

No stipulation.

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profile

7.1.1 Version number(s)

All participating CAs shall issue X.509 Version 3 certificates, in accordance with the PKIX Certificate and CRL Profile. The PKI end entity software shall support all the base (non-extension) X.509 fields as well as any certificate extensions defined in their CPS.

7.1.2 Certificate extensions

Certificate extensions will be supported by the CA in accordance with RFC 3280 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile" dated April 2002. All extensions used by the CA should be published in their CPS.

7.1.3 Algorithm object identifiers

All participating CAs shall use and end entities shall support, for signing and verification, the following:

1. RSA 1024 algorithm in accordance with PKCS#1 and/or
2. SHA-1 algorithm in accordance with FIPS PUB 180-1 and ANSI X9.30 part2 and/or
3. Additional algorithms as supported by the RSA Root Signing Service

7.1.4 Name forms

Every DN must be in the form of an ASN.1 X.501 DirectoryString

As stated in this CP in section 3.1.1.

7.1.5 Name constraints

Subject and Issuer DNs must comply with PKIX standards and be present in all certificates.

As stated in this CP in section 3.1.1.

7.1.6 Certificate policy object identifier

A Participating CA may have the Policy OID contained within the certificates it issues. These specifics will be identified in the CA's CPS.

7.1.7 Usage of Policy Constraints extension

A Participating CA may populate and mark as critical the policyConstraints extension.

7.1.8 Policy qualifiers syntax and semantics

A Participating CA may populate the CertificatePolicies extension with the OID identifier and policyQualifiers containing the URL of its CPS. User Notice Qualifier which point to an applicable Relying Party Agreement may be used at the discretion of the issuing CA.

7.1.9 Processing semantics for the critical Certificate Policies extension

Critical extensions shall be interpreted as defined in PKIX.

7.2 CRL profile

7.2.1 Version number(s)

All participating CAs shall issue X.509 version 2 CRLs in accordance with the RFC 3280 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile" dated April 2002. The PKI end entity software shall support all the base (non-extension) X.509 fields as well as any certificate extensions defined in the CPS.

7.2.2 CRL and CRL entry extensions

All entity PKI software shall correctly process all CRL extensions required in the PKIX Part 1 Certificate and CRL Profile. The CPS shall define the use of any extensions supported by the CA, its RAs and end entities.

7.3 OCSP profile

7.3.1 Version number(s)

Participating CA's OCSP responders shall implement Version 1 of the OCSP specification as defined by RFC2560 (X.509 Internet Public Key Infrastructure Online Certificate Status Protocol). The CPS will define the use of any extensions supported by the CA, its RAs and end entities.

7.3.2 OCSP extensions

The CA CPS shall define the use of any extensions supported by the CA, Subscribers and Relying Parties.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency or circumstances of assessment

All participating CAs will have an annual Compliance Audit performed by an independent, qualified third party at their own expense. The results of the annual Compliance Audit will be submitted to RSA Public Root CAs. The first Compliance Audit report must be submitted within six (6) months of the Certificate Signing Process and every twelve (12) months after the first Compliance Audit report.

The RSA ROOT SIGNING SERVICE will, at a minimum, certify annually that a Compliance Audit has been performed and that the CA has complied with the requirements of this policy. The annual Compliance Audit will determine whether the RSA Public Root CA's performance meets the standards established in its CPS and satisfies the requirements of the Certificate Policies it supports.

8.2 Identity/qualifications of assessor

The compliance auditor must demonstrate competence in the field of compliance audits, and must be thoroughly familiar with the requirements which the RSA ROOT SIGNING SERVICE imposes on the issuance and management of all certificates. The compliance auditor should perform such compliance audits as a primary responsibility.

The compliance auditor must be a practitioner who is approved by RSA ROOT SIGNING SERVICE to perform CA audits to verify and confirm compliance with this CP.

The minimal qualifications of an independent auditor shall be defined in the CA's CPS. If the CA is issuing EV certificates, the Compliance Auditor will be a qualified auditor as defined by the CA/Browser Forum's Guidelines for EV Certificates

8.3 Assessor's relationship to assessed entity

The Compliance Auditor should not have any financial, legal or organizational relationship with the audited party.

8.4 Topics covered by assessment

The purpose of a Compliance Audit shall be to verify that an entity subject to the requirements of this CP is complying with the requirements. The Compliance Audit will cover all requirements that define the operation of a CA under this CP including:

1. CA business practices disclosure
2. The RSA ROOT SIGNING SERVICE integrity (key and certificate life cycle management)
3. CA environmental controls

8.5 Actions taken as a result of deficiency

Depending on the severity of the deficiency, the following actions may be taken:

1. The Compliance Auditor may note the deficiency as part of the report.
2. The Compliance Auditor may meet with the CA and determine if the deficiency can be remedied, and an action plan should be developed and steps taken to remedy the deficiency.

3. The Compliance Auditor may report the deficiency and if the RSA ROOT SIGNING SERVICE deems the deficiency to have risk to the operation of the RSA Public Root CAs, the RSA ROOT SIGNING SERVICE operator may revoke the CA's certificate.

8.6 Communication of results

The Compliance Auditor shall provide the RSA ROOT SIGNING SERVICE management with a copy of the results of the Compliance Audit. The results will not be made public unless required by law.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

The charging of fees is subject to the appropriate authority and policy of the issuing Certification Authority. Notice of any fee charged to a Subscriber or Relying Party shall be brought to the attention of that entity.

9.1.1 Certificate issuance or renewal fees

No stipulation.

9.1.2 Certificate access fees

No stipulation.

9.1.3 Revocation or status information access fees

No stipulation.

9.1.4 Fees for other services

No stipulation.

9.1.5 Refund policy

No stipulation.

9.2 Financial responsibility

All participating CAs will maintain adequate levels of insurance necessary to support its business practices.

9.2.1 Insurance coverage

RSA shall maintain at its own expense insurance of the type necessary to meet its business requirements. Participating CAs shall maintain, at its own expense, insurance of the type and with the limits agreed upon within the RSA Root Signing agreement.

9.2.2 Other assets

No stipulation.

9.2.3 Insurance or warranty coverage for end-entities

RSA ROOT SIGNING SERVICE is not a trustee, agent, fiduciary, or other representative of the Subscriber and the relationship between the RSA ROOT SIGNING SERVICE and the Subscriber is not that of an agent and a principal. RSA ROOT SIGNING SERVICE makes no representation to the contrary, either implicitly, explicitly, by appearance or otherwise. The Subscriber does not have any authority to bind the RSA ROOT SIGNING SERVICE by contract, agreement or otherwise, to any obligation.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

Personal and corporate information, not appearing in certificates and in public directories, held by a CA or an RA (e.g. registration and revocation information, logged events, correspondence between Subscriber and CA) is considered confidential and shall not be disclosed by the CA or RA. Subscriber confidential information will not be disclosed without the prior consent of the Subscriber unless required by law.

Audit information is to be considered confidential and shall not be disclosed to anyone for any purpose other than audit purposes or where required by law, or a contractual agreement between the CA and the company being given access to the report that protects the confidentiality of the audit information.

Information pertaining to a CA's management of a Subscriber's digital signature certificate may only be disclosed to the Subscriber or where required by law.

Any request for the disclosure of information shall be signed and delivered in writing to the issuing Certification Authority.

Any disclosure of information is subject to the requirements of any privacy laws, the RSA ROOT SIGNING SERVICE Privacy Policy and any other relevant legislation and applicable organizational policy.

SIGNATURE

The digital signature private key of each Subscriber is to be held only by the Subscriber and shall be kept confidential by them. Any disclosure of the private key or media containing the private key by the Subscriber is at the Subscriber's own risk.

CONFIDENTIAL

The Subscriber shall keep the Subscriber's copy of their confidentiality private key confidential. Disclosure by the Subscriber is at the Subscriber's own risk. Confidentiality keys may be backed up by the issuing CA in which case these keys shall be protected in accordance with Section 6, and shall not be disclosed without prior consent of the Subscriber or a duly authorized representative of the issuing CA unless required by law.

9.3.2 Information not within the scope of confidential information

Certificates, OCSP responses, CRLs and personal or corporate information appearing in them and in public directories are not considered confidential information. Additionally, information that meets the following criteria shall not be considered to be confidential information:

1. Information that is documented by the receiving party as having been independently developed by it without unauthorized reference to or reliance on the confidential information of the disclosing party
2. Information that the receiving party lawfully receives free of restriction from a source other than the disclosing party
3. Information that is or becomes generally available to the public through no wrongful act or omission on the part of the receiving party
4. Information that at the time of disclosure to the receiving party was known to the receiving party free of restriction as evidenced by documentation in the receiving party's possession, or
5. Information that the disclosing party agrees in writing is free of restrictions

9.3.3 Responsibility to protect confidential information

A CA must ensure that confidential information be physically and/or logically protected from unauthorized viewing, modification or deletion. In addition, the CA must ensure that storage media used by the CA system is protected from environmental threats such as temperature, humidity and magnetism.

Confidentiality keys may be backed up by the issuing CA, in which case these keys shall be protected in accordance with Section 6, and shall not be disclosed without prior consent of the Subscriber or a duly authorized representative of the issuing CA unless required by law.

9.4 Privacy of personal information

9.4.1 Privacy plan

A CA's guiding principle is to not disclose private personal information of its Subscribers, customers, employees, and partners without the prior consent of the aforementioned unless required by law.

9.4.2 Information treated as private

Personal information, not appearing in certificates and in public directories, held by a CA or an RA (e.g. registration and revocation information, logged events, and correspondence between Subscriber and CA) is considered private, and shall not be disclosed by the CA or RA.

9.4.3 Information not deemed private

Personal information that is publicly available, or that appears in certificates and in public directories, is not considered private.

9.4.4 Responsibility to protect private information

A CA must ensure that private personal information be physically and/or logically protected from unauthorized viewing, modification or deletion. In addition, the CA must ensure that storage media used by the CA system is protected from environmental threats such as temperature, humidity and magnetism.

9.4.5 Notice and consent to use private information

Private personal information will only be utilized without prior consent as per section 9.4.1.

9.4.6 Disclosure pursuant to judicial or administrative process

Private personal information will only be disclosed if required by law as per section 9.4.1.

Any request for the disclosure of private information shall be signed by the requester and delivered in writing to the Participating CA. Any disclosure of private information is subject to the requirements of any privacy laws and any other relevant legislation and applicable organizational policy.

9.4.7 Other information disclosure circumstances

No stipulation.

9.5 Intellectual property rights

The private signing key shall be the sole property of the legitimate holder of the corresponding public key identified in a certificate.

Certification Authorities retain all intellectual property rights in and to the Certificates and revocation information that they issue. RSA and Customers shall grant permission to reproduce and distribute Certificates on a nonexclusive royalty-free basis, so long as they are reproduced in full and that use of Certificates is subject to the Relying Party Agreement referenced in the Certificate.

RSA retains all intellectual property rights in and to this CP.

9.6 Representations and warranties

A CA will issue and revoke certificates, operate its certification and repository services, and provide certificate status information in accordance with this CP.

Authentication and validation procedures will be implemented as set forth in Section 3 of this CP.

9.6.1 CA representations and warranties

All CAs will operate in accordance with this CP, their respective CPS(s) and applicable laws as described in Section 2.4.1, unless otherwise stipulated in the Root Signing Agreement, when issuing and managing certificates provided to CAs, RAs, sub-CAs and Subscribers under this CP. All participating CAs will require that all the RAs operating on their behalf will comply with the relevant provisions of this CP concerning the operations of the RAs. All participating CAs will take commercially reasonable measures to make Subscribers and Relying Parties aware of their respective rights and obligations with respect to the operation and management of any keys, certificates or End-Entity hardware and software used in connection with the PKI. Subscribers should also be notified as to procedures for dealing with suspected key compromise, certificate or key renewal, and service cancellation.

All Certification Authorities should provide notice of any limitation of liability (Section 2.2). Such notice may, at a minimum, be provided within the certificate either through a private certificate extension or the use of the "userNotice" field within the certificate as defined by PKIX. Because of space limitations within a certificate, such notice may be limited to the following language: "Limited Liability. See CP".

When a CA publishes or delivers a certificate, it declares that it has issued a certificate to a Subscriber and that the information stated in the certificate was verified in accordance with this CP.

CA personnel associated with PKI roles shall be individually accountable for actions they perform. "Individually accountable" means that there shall be evidence that attributes an action to the person performing the action.

9.6.2 RA representations and warranties

A CA shall require that all of its RA Administrators and Vectors comply with all the relevant provisions of this CP and the CA's CPS.

The RA Administrator or Vector is responsible for the identification and authentication of Subscribers following section 3.1 and section 4.1.

All participating CAs are required through their RA personnel to make available to Subscribers all relevant information pertaining to the rights and obligations of the CA, RA Administrators and

Vettors and Subscribers contained in this CP, the Subscriber agreement, if applicable, and any other relevant document outlining such terms and conditions.

The RA Administrator or Vettor is responsible for revoking certificates in accordance with Section 4.4.1 to Section 4.4.4.

RAs shall be individually accountable for actions performed on behalf of a CA. Individually accountability means that there must be evidence that attributes an action to the person performing the action (audit logs). Records of all actions carried out in performance of RA duties shall identify the individual who performed the particular duty.

When an RA submits Subscriber information to a CA, it shall certify to that CA that it has authenticated the identity of that Subscriber and that the Subscriber is authorized to submit a certificate request in accordance with Section 3 and Section 4.

Submission of the certificate request to the CA is to be performed in a secure manner as described in section 3.1.

9.6.3 Subscriber representations and warranties

Subscribers are required to protect their private keys, associated pass phrase(s) and tokens, as applicable, in accordance with Section 6, and to take all commercially reasonable measures to prevent their loss, disclosure, modification, or unauthorized use

Any Subscriber information shall be complete, validated and accurate with full disclosure of all required information in connection with a certificate or a query to a CA.

The Subscriber shall only use the keys and certificates for the purposes identified in this CP and in any applicable agreement(s).

When a Subscriber suspects a private key compromise, the Subscriber shall notify the issuing Certification Authority in the manner specified by Section 4.4.3. When any other entity suspects private key compromise, they should notify the issuing CA

9.6.4 Relying party representations and warranties

The rights and obligations of a Relying Party who is a Subscriber of a CA within the RSA ROOT SIGNING SERVICE are covered in this policy. The rights and obligations of a Relying Party belonging to another PKI shall be addressed in the cross certification process or some other approved agreement.

Prior to using a Subscriber's certificate, a Relying Party should verify that the certificate is appropriate for the intended use.

A Relying Party should use certificates only in accordance with the certification path validation procedure specified in X.509 and PKIX.

Prior to using a certificate, a Relying Party should check the status of the certificate against the appropriate and current CRL or OCSP Responder in accordance with the requirements stated in Sections 4.4.10 and 4.4.11. As part of this verification process the digital signature of the CRL or OCSP Responder should also be validated.

9.6.5 Representations and warranties of other participants

No stipulation.

9.7 Disclaimers of warranties

The RSA Public Root CAs assumes no liability except as stated in the relevant contracts pertaining to certificate issuance and management, such as the Root Signing Agreement, a Subscriber Agreement or other relevant customer contract.

NEITHER RSA SECURITY NOR THE RSA ROOT SIGNING SERVICE THEREBY MAKE OR GIVE, AND HEREBY EXPRESSLY DISCLAIMS, ALL WARRANTIES, REPRESENTATIONS, OR CONDITIONS, BOTH EXPRESS AND IMPLIED, ARISING BY STATUE OR OTHERWISE IN LAW, OR FROM A COURSE OF DEALING OR USAGE OR TRADE, INCLUDING, BUT NOT LIMITED TO, AN IMPLIED WARRANTY, REPRESENTATION, OR CONDITION OF MERCHANTABILITY, MERCHANTABLE QUALITY, OR FITNESS FOR ANY PURPOSE, PARTICULAR, SPECIFIC, OR OTHERWISE, OR ANY WARRANTY OF TITLE OR NON-INFRINGEMENT, FOR ANY OF THE PRODUCTS, SERVICES, PROGRAMS, SPECIFICATIONS, STANDARDS, SOFTWARE, HARDWARE, OR FIRMWARE CREATED, SUPPLIED, REQUIRED, LICENSED, OR APPROVED BY RSA SECURITY, OR REFERENCED IN THE OPERATIONAL REGULATIONS OR OPERATING PRINCIPLES OF SUCH OR THIS CERTIFICATE POLICY.

IN NO EVENT SHALL THE RSA ROOT SIGNING SERVICE BE LIABLE TO ANY PARTY FOR ANY INCIDENTAL, CONSEQUENTIAL, SPECIAL, INDIRECT OR PUNITIVE DAMAGES, LOST BUSINESS PROFITS, OR LOSS, DAMAGE OR DESTRUCTION OF DATA ARISING OUT OF OR RELATED IN ANY WAY TO THE CERTIFICATES ISSUED BY THE RSA PUBLIC ROOT CA V1, REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), BREACH OF WARRANTY, OR OTHERWISE, EVEN IF THE RSA PUBLIC ROOT CA V1 HAS BEEN ADVISED OF THE POSSIBILITY OF THE SAME.

Nothing in this CP shall confer on any third party any authority to act for, bind, or create or assume any obligation or responsibility, or make any representation on behalf of another except as set forth in a relevant contract. Issuance of certificates in accordance with this policy does not make a CA or any RA an agent, partner, joint venture, fiduciary, trustee or other representative of Subscribers, customers or other Relying Parties. The relationship between a CA, any RA and the Subscriber is defined by an applicable contract between those parties.

The disclaimers may be superseded by terms of a signed contract that may be entered into by the RSA ROOT SIGNING SERVICE that provide otherwise.

9.8 Limitations of liability

In no event will RSA Security or the RSA ROOT SIGNING SERVICE be liable for any damages to Subscribers, Relying Parties or any other party arising out of or related to the misuse of, or reliance on Certificates issued by a CA that have been:

1. Revoked or expired
2. Used for unauthorized purposes
3. Tampered with
4. Compromised
5. Subject to misrepresentation, misleading acts or omissions

The limitations of liability may be superseded by terms of a signed contract that may be entered into by the RSA ROOT SIGNING SERVICE that provide otherwise.

IN NO EVENT WILL RSA SECURITY OR RSA SECURITY'S LICENSORS OR SUPPLIERS BE LIABLE FOR INCIDENTAL, CONSEQUENTIAL, SPECIAL OR INDIRECT DAMAGES, LOST BUSINESS PROFITS, OR LOSS, DAMAGE OR DESTRUCTION OF DATA, REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), BREACH OF WARRANTY OR OTHERWISE, EVEN IF RSA SECURITY OR RSA SECURITY'S

LICENSORS OR SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF THE SAME. NO LIMITATION AS TO DAMAGES FOR PERSONAL INJURY IS HEREBY INTENDED.

9.9 Indemnities

Unless otherwise set forth in this CP/CPS and/or Subscriber Agreement and/or Relying Party Agreement and/or RSA Root Signing Agreement, Subscriber and/or Relying Party hereby agrees to indemnify and hold RSA ROOT Signing Service harmless from any claims, actions or demands that arise from the use or publication of a certificate, and:

1. Any false or misleading statement of fact by the Subscriber
2. Any failure by the Subscriber to disclose a material fact, regardless if such omission was made negligently or with the intent to deceive
3. Any failure on the part of the Subscriber to protect its Private Key and/or token if applicable, or to take the precautions necessary to prevent the compromise, disclosure, loss, modification or unauthorized use of the Subscriber's private key, or
4. Any failure on the part of the Subscriber to promptly notify the RSA PUBLIC ROOT CA V1 of the compromise, disclosure, loss, modification or unauthorized use of the Subscriber's private key once the Subscriber has actual or constructive notice of such event.

9.10 Term and termination

9.10.1 Term

This CP remains in force until notice of the opposite is communicated by RSA Security on its web site in the Root Signing Service Repository (<http://www.rsasecurity.com/node.asp?id=2420>).

9.10.2 Termination

Termination of this document will be upon publication of a newer version or replacement document, or upon termination of CA operations.

9.10.3 Effect of termination and survival

The conditions and effect resulting from termination of this document will be communicated, on RSA Security's web site in the Root Signing Service Repository (<http://www.rsasecurity.com/node.asp?id=2420>), upon termination outlining the provisions that may survive termination of the document and remain in force.

9.11 Individual notices and communications with participants

The RSA ROOT SIGNING SERVICE will define in any applicable agreement the appropriate provisions governing notices.

9.12 Amendments

RSA Security Policy Management Authority is the responsible authority for reviewing and approving changes to this CP. Written and signed comments on proposed changes shall be directed to the RSA ROOT SIGNING SERVICE contact as described in Section 1.5. Decisions with respect to the proposed changes are at the sole discretion of the RSA Security Policy Management Authority.

9.12.1 Procedure for amendment

CRL publication shall be in accordance with Section 2 and 4. A Participating CA under the ROOT SIGNING SERVICE shall provide full text version of this CP and their CPS when necessary for the purposes of audit, accreditation or as required by law.

An electronic copy of RSA RSS CP is to be made available at the RSA Security web site http://rsasecurity.com/products/keon/repository/practices/Certificate_Policy.pdf or by requesting an electronic copy by e-mail to the contact representative as described in Section 1.5.

The RSA Security Policy Management Authority may provide notice, in writing, of any proposed changes to the RSA RSS CP, if in the judgment and discretion of RSA Security Policy Management Authority the changes may have significant impact on the issued certificates, or PKI services.

The period of time that affected parties have to conform to the change will be defined in the notification.

9.12.2 Notification mechanism and period

The notification shall contain a statement of proposed changes, the final date for receipt of comments, and the proposed effective date of the changes. The RSA Security Policy Management Authority will post the notification at the CP publishing point at <http://www.rsasecurity.com/node.asp?id=2420>.

The comment period will be 30 days unless otherwise specified.

9.12.3 Circumstances under which OID must be changed

If a policy change is determined by the RSA Security Policy Management Authority to warrant the issuance of a new policy, the RSA Security Policy Management Authority will assign a new Object Identifier (OID) for the new policy.

9.13 Dispute resolution provisions

Any dispute related to key and certificate management between a CA and any other organization or individual outside that CA should be resolved using an appropriate dispute resolution mechanism. A dispute should be resolved by negotiations if possible. Each CA shall define an appropriate dispute resolution procedure in any agreement it enters into.

Any dispute with the RSA Public Root v1 not resolved by negotiations shall be brought before the courts of the Commonwealth of Massachusetts, or as otherwise agreed to in writing by RSA Security.

A dispute resolution process will be described in the CA's CPS and any applicable agreements.

9.14 Governing law

This CP and all corresponding agreements shall be governed by the laws of the Commonwealth of Massachusetts, or as otherwise agreed to in writing by RSA Security, without regard to its conflict of laws principles.

9.15 Compliance with applicable law

This CP is subject to applicable national, state, local and foreign laws, rules, regulations, ordinances, decrees and orders including but not limited to restrictions on exporting or importing software, hardware or technical information.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

The RSA ROOT SIGNING SERVICE will define in any applicable agreement the appropriate provisions governing severability and survival of clauses, assignment of the agreement and notice requirements.

9.16.2 Assignment

Subscribers and Relying Parties may not assign any of their rights or obligations under their applicable agreements, without the written consent of RSA ROOT SIGNING SERVICE.

9.16.3 Severability

The RSA ROOT SIGNING SERVICE will define in any applicable agreement the appropriate provisions governing severability.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

The RSA ROOT SIGNING SERVICE will define in any applicable agreement the appropriate provisions governing Enforcement.

9.16.5 Force Majeure

The RSA ROOT SIGNING SERVICE shall not be held responsible for any delay or failure in performance of its obligations hereunder to the extent such delay or failure is caused by fire, flood, strike, civil, governmental or military authority, acts of terrorism or war, act of God, or other similar causes beyond its reasonable control and without the fault or negligence of the RSA Root Signing Service or its subcontractors.

9.17 Other provisions

No stipulation.

ACRONYMS

ASN.1	Abstract Syntax Notation number one
CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DER	Distinguished Encoding Rules
DN	Distinguished Name
DSA	Digital Signature Algorithm
EAL	Evaluation Assurance Level
EV	Extended Validation
FIPS	Federal Information Processing Standard
HSM	Hardware Security Module
IETF	Internet Engineering Task Force
ITU	International Telecommunications Union
LDAP	Lightweight Directory Access Protocol
MD5	Message Digest 5
OCSP	Online Certificate Status Protocol
PIN	Personal Identification Number
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
RA	Registration Authority
RFC	Request for Comment
RSA	Rivest-Shamir-Adleman
SHA –1	Secure Hash Algorithm
S/MIME	Secure Multipurpose Internet Mail Extension
SSL	Secure Sockets Layer
UPS	Uninterruptible Power Supply
URI	Uniform Resource Identifier
URL	Uniform Resource Locator

GLOSSARY

A

TERM: access control

DEFINITION: The granting or denial of use or entry.

TERM: Activation Data

DEFINITION: Activation data, in the context of certificate enrollment, consists of a one-time secret communicated to the enrolling user (Subscriber) out of band. This shared secret permits the user to complete of the enrollment process.

TERM: Administrator

DEFINITION: A Trusted Person within the organization of a Processing Center, Service Center, Managed PKI Customer, or Gateway Customer that performs validation and other CA or RA functions.

TERM: Administrator Certificate

DEFINITION: A Certificate issued to an Administrator that may only be used to perform CA or RA functions.

TERM: Agent

DEFINITION: A person, contractor, service provider, etc. that is providing a service to <ORGNAME> under contract and are subject to the same corporate policies as if they were an employee of <ORGNAME>.

TERM: Application Server

DEFINITION: An application service that is provided to <ORGNAME> or one of its partners and may own a certificate issued under the <ORGNAME> PKI. Examples are Web SSL servers, VPN servers (IPSec), object signer services, Domain Controllers, etc.

TERM: authentication

DEFINITION: The act of verifying; in the case of identities, the assurance of an identity.

TERM: authorization

DEFINITION: The granting of permissions of use.

B

TERM: business process

DEFINITION: A set of one or more linked procedures or activities which collectively realize a business objective or policy goal, normally within the context of an organizational structure defining functional roles and relationships.

C

TERM: certificate

DEFINITION: The public key of a user, together with related information, digitally signed with the private key of the Certification Authority that issued it. The certificate format is in accordance with ITU-T Recommendation X.509.

TERM: Certification Authority (CA)

DEFINITION: An authority trusted by one or more users to manage X.509 certificates and CRLs.

TERM: CA (Certification Authority) room / facility

DEFINITION: The room or facility where the CA systems and components are enclosed, and which the <ORGNAME> PKI Policy Management Authority has control regarding who has access to this room or facility.

TERM: Certification Chain

DEFINITION: An ordered list of Certificates containing an end-user Subscriber Certificate and CA Certificates, which terminates in a root Certificate.

TERM: Certificate Policy

DEFINITION: Named set of rules that indicates the applicability of a certificate to a particular community and/or class of applications with common security requirements. It is the principal statement of certificate policy governing the <ORGNAME> PKI. The CP is a high-level document that describes the requirements, terms and conditions, and policy for issuing, utilizing and managing certificates issued by a CA.

TERM: Certification Practice Statement

DEFINITION: A statement of the practices, which a Certification Authority employs in issuing certificates. It is a comprehensive description of such details as the precise implementation of service offerings and detailed procedures of certificate life-cycle management and will be more detailed than the certificate policies supported by the CA.

TERM: Certificate Revocation List

DEFINITION: A periodically issued list, digitally signed by a CA, of identified Certificates that have been revoked prior to their expiration dates. The list generally indicates the CRL issuer's name, the date of issue, the date of the next scheduled CRL issue, the revoked Certificates' serial numbers, and the specific times and reasons for revocation. CRL can be used to check the status of certificates.

TERM: Common Criteria

DEFINITION: The Common Criteria is an Internal agreed upon IT Security evaluation criteria. It represents the outcome of a series of efforts to develop criteria for evaluation of IT security that are broadly useful within the international community.

TERM: confidential

DEFINITION: A security classification used to describe information which if disclosed could result in personal loss or minor financial loss. Personal information and tactical information would be deemed confidential.

TERM: Confidentiality

DEFINITION: Information that has an identifiable value associated with it such that if disclosed might cause damage to an entity.

TERM: Cross Certification

DEFINITION: The process describing the establishing of trust between two or more CAs. Usually involves the exchange and signing of CA certificates and involves the verification of assurance levels.

D

TERM: Distinguished Encoding Rules (DER)

DEFINITION: The Distinguished Encoding Rules for ASN.1, abbreviated DER, gives exactly one way to represent any ASN.1 value as an octet string. DER is intended for applications in which a unique octet string encoding is needed, as is the case when a digital signature is computed on an ASN.1 value.

TERM: Digital Signature

DEFINITION: The result of the transformation of a message by means of a cryptographic system using keys such that a person who has the initial message can determine that the key that corresponds to the signer's key created the transformation and the message was not altered.

TERM: Distinguished Name (DN)

DEFINITION: Every entry in a X.500 or LDAP directory has a Distinguished Name, or DN. It is a unique entry identifier through out the complete directory. No two Entries can have the same DN within the same directory. A DN is used in certificates to uniquely identify a certificate-owner.

Example of a DN:

```
cn=Road Runner, ou=bird, dc=carton, dc=com
ou=bird, dc=carton, dc=com
dc=carton, dc=com
dc=com
```

TERM: Dual Control

DEFINITION: A process utilizing two or more separate entities (usually persons), operating in concert, to protect sensitive functions or information, whereby no single entity is able to access or utilize the materials, e.g., cryptographic key.

E

TERM: E-mail Certificates

DEFINITION: Certificates utilized for encrypting and verifying digital signatures. Normally two separate certificate: one for encryption, the other for signature verification.

TERM: Entity

DEFINITION: Any autonomous element or component within the Public Key Infrastructure that participate is one form or another, such managing certificates or utilizing certificates. An Entity can be a CA, RA, Subscriber, Relying Party, etc.

F

TERM: FIPS 140-2

DEFINITION: Federal Information Processing Standard 140-2(FIPS 140-2) is a standard that describes US Federal government requirements that IT products shall meet for Sensitive, but Unclassified (SBU) use. The standard was published by the National Institute of Standards and Technology (NIST), has been adopted by the Canadian government's Communication Security Establishment (CSE), and is likely to be adopted by the financial community through the American National Standards Institute (ANSI). The different levels (1 to 4) within the standard provide different levels of security and in the higher levels have different documentation requirements.

TERM: FIPS 180-1

DEFINITION: Standard specifying a Secure Hash Algorithm, SHA-1, for computing a condensed representation of a message or a data files.

G

H

I

TERM: Integrity

DEFINITION: Ensuring consistency of an object or information. Within security systems, integrity is the principle of ensuring that a piece of data has not been modified maliciously or accidentally.

TERM: ISO 9564-1

DEFINITION: Basic principles and requirements for online PIN handling in ATM and POS systems, provides instructions to financial institutions in the development, implementation and/or the operation of systems and procedures for the protection of PIN throughout its lifecycle.

TERM: ISO 11568-5

DEFINITION: Basic principles and requirements for Key lifecycle for public key cryptosystems, provides instructions to financial institutions in the development, implementation and/or the operation of systems and procedures throughout Key's lifecycle.

J**K****TERM: Key**

DEFINITION: When used in the context of cryptography, it is a secret value, a sequence of characters that is used to encrypt and decrypt data. A key is a unique, generated electronic string of bits used for encrypting, decrypting, e-signing or validating digital signatures.

TERM: Key Pair

DEFINITION: Often referred to as public/private key pair. One key is used for encrypting and the other key used for decrypting. Although related, the keys are sufficiently different that knowing one does not allow derivation or computation of the other. This means that one key can be made publicly available without reducing security, provided the other key remains private.

L**M****TERM: MD5**

DEFINITION: One of the message digest algorithms developed by RSA.

N**TERM: non-repudiation**

DEFINITION: Protection against the denial of the transaction or service or activity occurrence.

O**TERM: Object Identifier**

DEFINITION: The unique alpha-numeric identifier registered under the ISO registration standard to reference a standard object or class.

P**TERM: PKCS #1**

DEFINITION: Standard that provides recommendations for the implementation of public-key cryptography based on the RSA algorithm, covering the following aspects: cryptographic primitives; encryption schemes; signature schemes, etc.

TERM: PKCS #7

DEFINITION: A cryptographic message format or syntax managed and edited by RSA Laboratories. A standard describing general syntax for data that may have cryptography applied to it, such as digital signatures and digital envelopes.

TERM: PKCS #10

DEFINITION: A certificate request format or syntax managed and edited by RSA Laboratories. It is a standard describing syntax for a request for certification of a public key, a name, and possibly a set of attributes.

TERM: PKIX

DEFINITION: The Public Key Infrastructure (X.509) or PKIX is an IETF Working Group established with the intent of developing Internet standards needed to support an X.509-based PKI. The scope of PKIX extends to also develop new standards for use of X.509-based PKIs in the Internet.

TERM: PKI personnel

DEFINITION: Persons, generally employees, associated with the operation, administration and management of a CA or RA.

TERM: policy

DEFINITION: The set of laws, rules and practices that regulates how an organization manages its business. Specifically, security policy would be the set of laws, rules and practices that regulates how an organization manages, protects and distributes sensitive information.

TERM: PrintableString

DEFINITION: String format for representing names, such as Common Name (CN), in X.509 certificates. The encoding of a value in this syntax is the string value itself.

TERM: Private Key

DEFINITION: The private key is one of the keys in a public/private key pair. This is the key that is kept secret as opposed to the other key that is publicly available. Private keys are utilized for digitally signing documents, uniquely authenticating an individual, or decrypting data that was encrypted with the corresponding public key.

TERM: Public Key Infrastructure

DEFINITION: A set of policies, procedures, technology, audit and control mechanisms used for the purpose of managing certificates and keys.

TERM: Public

DEFINITION: A security classification for information that if disclosed would not result in any personal damage or financial loss.

TERM: Public Key

DEFINITION: The community verification key for digital signature and the community encryption key for encrypting information to a specific Subscriber.

Q

R

TERM: Registration Authority

DEFINITION: An entity that performs registration services on behalf of a CA. RAs work with a particular CA to vet requests for certificates that will then be issued by the CA.

TERM: Rekey

DEFINITION: The process of replacing or updating the key(s). The expiration of the crypto period involves the replacement of the public key in the certificate and therefore the generation of a new certificate. <ORGNAMES> PKI does not support rekey.

TERM: Relative Distinguished Name (RDN)

DEFINITION: A Distinguished Name is made up of a sequence of Relative Distinguished Names, or RDNs. The sequences of RDNs are separated by commas (,) or semi-colons (;). There can be more than one identical RDN in a directory, but they must be in different bases, or branches, of the directory. Example of a DN is "cn=Road Runner,ou=bird,dc=carton,dc=com"

RDNs would be:

RDN => cn=Road Runner

RDN => ou=bird

RDN => dc=carton

RDN => dc=com

TERM: Relying Party

DEFINITION: A person or entity that uses a certificate signed by the CA to authenticate a digital signature or encrypt communications to a certificate subject. The relying party relies on the

certificate as a result of the certificate being signed by a CA, which is trusted. A relying party normally is but does not have to be a Subscriber of the PKI.

TERM: Repository

DEFINITION: A place or container where objects are stored. A data repository is technology where data is stored logically. In PKI terms, a repository accepts certificates and CRLs from one or more CAs and makes them available to entities that need them for implementing security services.

TERM: Revocation

DEFINITION: In PKI, revocation is the action associated with revoking a certificate. Revoking a certificate is to make the certificate invalid before its normal expiration. The Certification Authority that issued the certificate is the entity that revokes a certificate. The revoked status is normally published on a certificate revocation list (CRL).

TERM: RSA

DEFINITION: A public key cryptographic algorithm invented by Rivest, Shamir, and Adelman..

S**TERM: Sensitive**

DEFINITION: Used to describe the security classification of information where the information if disclosed would result in serious financial loss, serious loss in confidence or could result in personal harm or death.

TERM: Signature Verification Certificate

DEFINITION: Often referred to as simply a Signature Certificate. It is the certificate containing the public key used to verify a digital signature that was signed by the corresponding private key.

TERM: Split Knowledge

DEFINITION: A condition under which two or more parties separately and confidentially have custody of components of a single key that, individually, convey no knowledge of the resultant cryptographic key. The resultant key exists only within secure cryptographic devices.

TERM: SSL Client Certificate

DEFINITION: Certificate utilized to verify the authentication of an end user to a server when a connection is being established via a SSL session (secure channel)..

TERM: SSL Server Certificate

DEFINITION: Certificate utilized to verify the authentication of a web or application server to the end user (client) when a connection is being established via a SSL session (secure channel).

TERM: Subscriber

DEFINITION: A Subscriber is an entity; a person or application server that is a holder of a private key corresponding to a public, and has been issued a certificate. In the case of an application server, a person authorized by the organization owning the application server may be referred to as the Subscriber. A Subscriber is capable of using, and is authorized to use, the private key that corresponds to the public key listed in the certificate.

TERM: Surveillance Camera

DEFINITION: A surveillance camera is a video recording device used for detection and identification of unauthorized physical entry to a secured area. A camera used for recording a signing ceremony for auditing purposes is not considered a surveillance camera.

T**TERM: threat**

DEFINITION: A danger to an asset in terms of that asset's confidentiality, integrity, availability or legitimate use.

TERM: Token

DEFINITION: Hardware devices normally associated with a reader, used to store and/or generate encryption keys, such as smartcards and USB tokens.

U

TERM: URI

DEFINITION: Universal Resource Indicator - an address on the Internet.

TERM: UTF8String

DEFINITION: A UTF-8 is a type of Unicode, which is a character set supported across many commonly used software applications and operating systems. UTF-8 is a multibyte encoding in which each character can be encoded in as little as one byte and as many as four bytes. Most Western European languages require less than two bytes per character. Greek, Arabic, Hebrew, and Russian require an average of 1.7 bytes. Japanese, Korean, and Chinese typically require three bytes per character. Such Unicode is important to ensure universal character / foreign characters are supported.

V

TERM: Valid Business Relationship

DEFINITION: A relationship between <ORGNAME> and an <ORGNAME>' partner, supplier, member or other business affiliation, or an agent representing an <ORGNAME>' partner, supplier, member or other business affiliation, or an approved contractor; and a have a requirement to access <ORGNAME>' electronic services. An Electronic Access Agreement will be in place with the organization representing this relationship.

TERM: Vettor

DEFINITION: A person who verifies information provided by a person applying for a certificate.

TERM: vulnerability

DEFINITION: Weaknesses in a safeguard or the absence of a safeguard.

W

X

TERM: X.500

DEFINITION: Specification of the directory service required to support X.400 e-mail initially but common used by other applications as well.

TERM: X501PrintableString

DEFINITION: String format for representing names, such as Common Name (CN), in X.509 certificates. The encoding of a value in this syntax is the string value itself; an arbitrary string of printable characters.

TERM: X.509

DEFINITION: An ISO standard that describes the basic format for digital certificates.

Y

Z