
VeriSign Trust Network Certificate Policies



Version 1.3

Effective Date: March 31, 2004



VeriSign, Inc.
487 E. Middlefield Road
Mountain View, CA 94043 USA
+1 650.961.7500
<http://www.verisign.com>

VeriSign Trust Network Certificate Policies

© 2004 VeriSign, Inc. All rights reserved.
Printed in the United States of America.

Revision date: March 31, 2004

Trademark Notices

VeriSign and OnSite are registered trademarks of VeriSign, Inc. The VeriSign logo, VeriSign Trust Network, NetSure, and Go Secure! are trademarks and service marks of VeriSign, Inc. Other trademarks and service marks in this document are the property of their respective owners.

Without limiting the rights reserved above, and except as licensed below, no part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), without prior written permission of VeriSign, Inc.

Notwithstanding the above, permission is granted to reproduce and distribute these VeriSign Certificate Policies on a nonexclusive, royalty-free basis, provided that (i) the foregoing copyright notice and the beginning paragraphs are prominently displayed at the beginning of each copy, and (ii) this document is accurately reproduced in full, complete with attribution of the document to VeriSign, Inc.

Requests for any other permission to reproduce these VeriSign Certificate Policies (as well as requests for copies from VeriSign) must be addressed to VeriSign, Inc., 487 E. Middlefield Road, Mountain View, CA 94043 USA Attn: Practices Development. Tel: +1 650.961.7500 Fax: +1 650.426.7300 Net: **practices@verisign.com**.

Acknowledgement

VeriSign acknowledges the invaluable assistance of J.F. Sauriol of Labcal Technologies Inc. (<http://www.labcal.com>) regarding technical elements and structure of the VeriSign Trust Network Certificate Policies. VeriSign also acknowledges the assistance of many reviewers of the document specializing in diverse areas of business, law, policy, and technology.

TABLE OF CONTENTS

1. Introduction	1
1.1 Overview	1
1.1.1 Policy Overview	7
1.1.2 VTN Suite of Services	10
1.1.2.1 Certificate Distribution Services	10
1.1.2.1.1 VeriSign Managed PKI [®]	10
1.1.2.1.2 VeriSign Affiliate Program	12
1.1.2.1.3 Universal Service Center Program and Other Reseller Programs	14
1.1.2.1.4 The Web Host Program	14
1.1.2.1.5 VeriSign Gateway Services	15
1.1.2.2 Value-Added Certification Services	15
1.1.2.2.1 Authentication Services	15
1.1.2.2.2 VeriSign Digital Notarization Service	16
1.1.2.2.3 NetSure SM Protection Plan	17
1.1.2.3 Special Certificate Types	17
1.1.2.3.1 Wireless Certificate Services	17
1.1.2.3.2 VeriSign Managed PKI Key Manager Services	18
1.1.2.3.3 VeriSign Roaming Service	19
1.2 Identification	19
1.3 Community and Applicability	19
1.3.1 Certification Authorities	20
1.3.2 Registration Authorities	21
1.3.3 End Entities	21
1.3.4 Applicability	22
1.3.4.1 Suitable Applications	23
1.3.4.1.1 Class 1 Certificates	23
1.3.4.1.2 Class 2 Certificates	24
1.3.4.1.3 Class 3 Certificates	24
1.3.4.1.3.1 Class 3 Individual Certificates	24
1.3.4.1.3.2 Class 3 Organizational Certificates	24
1.3.4.2 Restricted Applications	26
1.3.4.3 Prohibited Applications	26
1.4 Contact Details	27
1.4.1 Specification Administration Organization	27
1.4.2 Contact Person	27
1.4.3 Person Determining CPS Suitability for the Policy	27
2. General Provisions	27
2.1 Obligations (Class 1-3)	27
2.1.1 CA Obligations	27
2.1.2 RA Obligations	28
2.1.3 Subscriber Obligations	28
2.1.4 Relying Party Obligations	29
2.1.5 Repository Obligations	29

2.2	Liability (Class 1-3)	30
2.2.1	Certification Authority Liability	30
2.2.1.1	Certification Authority Warranties to Subscribers and Relying Parties	31
2.2.1.2	Certification Authority Disclaimers of Warranties	32
2.2.1.3	Certification Authority Limitations of Liability	32
2.2.1.4	Force Majeure	32
2.2.2	Registration Authority Liability	32
2.2.3	Subscriber Liability	33
2.2.3.1	Subscriber Warranties	33
2.2.3.2	Private Key Compromise	33
2.2.4	Relying Party Liability	34
2.3	Financial Responsibility (Class 1-3)	34
2.3.1	Indemnification by Subscribers and Relying Parties	34
2.3.1.1	Indemnification by Subscribers	34
2.3.1.2	Indemnification by Relying Parties	34
2.3.2	Fiduciary Relationships	34
2.3.3	Administrative Processes	35
2.4	Interpretation and Enforcement (Class 1-3)	35
2.4.1	Governing Law	35
2.4.2	Severability, Survival, Merger, Notice	35
2.4.3	Dispute Resolution Procedures	35
2.4.3.1	Disputes Among VeriSign, Affiliates, and Customers	35
2.4.3.2	Disputes with End-User Subscribers or Relying Parties	36
2.5	Fees (Class 1-3)	36
2.5.1	Certificate Issuance or Renewal Fees	36
2.5.2	Certificate Access Fees	36
2.5.3	Revocation or Status Information Access Fees	36
2.5.4	Fees for Other Services Such as Policy Information	36
2.5.5	Refund Policy	36
2.6	Publication and Repository (Class 1-3)	37
2.6.1	Publication of CA Information	37
2.6.1.1	Publication by VeriSign and Affiliates	37
2.6.1.2	Publication by Gateway Customers	37
2.6.2	Frequency of Publication	37
2.6.3	Access Controls	37
2.6.4	Repositories	38
2.7	Compliance Audit	38
2.7.1	Frequency of Entity Compliance Audit (Class 1-3)	38
2.7.2	Identity/ Qualifications of Auditor	38
2.7.2.1	Personnel Performing Self-Audits (Class 1-3)	39
2.7.2.2	Qualifications of Third-Party Audit Firms (Class 1-3)	39
2.7.3	Auditor's Relationship to Audited Party (Class 1-3)	39
2.7.4	Topics Covered by Audit	39
2.7.4.1	Self-Audits of Gateway Customers (Class 1)	39
2.7.4.2	Self-Audits of Managed PKI Customers (Class 1-2)	40
2.7.4.3	Audit of an Managed PKI Customer (Class 3)	40

2.7.4.4	Audit of VeriSign or an Affiliate (Class 1-3)	40
2.7.5	Actions Taken as a Result of Deficiency (Class 1-3)	40
2.7.6	Communications of Results (Class 1-3)	41
2.8	Confidentiality and Privacy (Class 1-3)	41
2.8.1	Types of Information to be Kept Confidential and Private	41
2.8.2	Types of Information Not Considered Confidential or Private	41
2.8.3	Disclosure of Certificate Revocation/Suspension Information	41
2.8.4	Release to Law Enforcement Officials	42
2.8.5	Release as Part of Civil Discovery	42
2.8.6	Disclosure Upon Owner's Request	42
2.8.7	Other Information Release Circumstances	42
2.9	Intellectual Property Rights (Class 1-3)	42
2.9.1	Property Rights in Certificates and Revocation Information	42
2.9.2	Property Rights in the CP	42
2.9.3	Property Rights in Names	43
2.9.4	Property Rights in Keys and Key Material	43
3.	Identification and Authentication	43
3.1	Initial Registration	43
3.1.1	Types of Names (Class 1-3)	43
3.1.2	Need for Names to be Meaningful (Class 1-3)	43
3.1.3	Rules for Interpreting Various Name Forms (Class 1-3)	44
3.1.4	Uniqueness of Names (Class 1-3)	44
3.1.5	Name Claim Dispute Resolution Procedure (Class 1-3)	44
3.1.6	Recognition, Authentication, and Role of Trademarks (Class 1-3)	44
3.1.7	Method to Prove Possession of Private Key (Class 1-3)	44
3.1.8	Authentication of Organization Identity	44
3.1.8.1	Authentication of the Identity of Organizational End-User Subscribers (Class 3)	44
3.1.8.1.1	Authentication for Retail Organizational Certificates	45
3.1.8.1.2	Authentication for Managed PKI for SSL or Managed PKI for SSL Premium Edition	45
3.1.8.1.3	Authentication for Class 3 Organizational ASB Certificates	45
3.1.8.2	Authentication of the Identity of CAs and RAs (Class 1-3)	46
3.1.9	Authentication of Individual Identity	47
3.1.9.1	Class 1 Certificates	47
3.1.9.2	Class 2 Certificates	48
3.1.9.2.1	Class 2 Managed PKI Certificates	48
3.1.9.2.2	Class 2 Retail Certificates	48
3.1.9.3	Class 3 Individual Certificates	48
3.2	Routine Rekey (Renewal) (Class 1-3)	49
3.2.1	Renewal of End-User Subscriber Certificates	49
3.2.2	Renewal of CA Certificates	50
3.3	Rekey After Revocation (Class 1-3)	50
3.4	Revocation Request (Class 1-3)	50
4.	Operational Requirements	51
4.1	Certificate Application (Class 1-3)	51

4.1.1	Certificate Applications for End-User Subscriber Certificates.....	51
4.1.2	Certificate Applications for CA or RA Certificates.....	52
4.2	Certificate Issuance (Class 1-3)	53
4.2.1	Issuance of End-User Subscriber Certificates.....	53
4.2.2	Issuance of CA and RA Certificates	53
4.3	Certificate Acceptance (Class 1-3)	54
4.4	Certificate Suspension and Revocation (Class 1-3).....	54
4.4.1	Circumstances for Revocation	54
4.4.1.1	Circumstances for Revoking End-User Subscriber Certificates.....	54
4.4.1.2	Circumstances for Revoking CA or RA Certificates.....	55
4.4.2	Who Can Request Revocation	56
4.4.2.1	Who Can Request Revocation of an End-User Subscriber Certificate.....	56
4.4.2.2	Who Can Request Revocation of a CA or RA Certificate.....	56
4.4.3	Procedure for Revocation Request.....	56
4.4.3.1	Procedure for Requesting the Revocation of an End-User Subscriber Certificate 56	
4.4.3.2	Procedure for Requesting the Request Revocation of a CA or RA Certificate	56
4.4.4	Revocation Request Grace Period	57
4.4.5	Circumstances for Suspension	57
4.4.6	Who Can Request Suspension	57
4.4.7	Procedure for Suspension Request.....	57
4.4.8	Limits on Suspension Period	57
4.4.9	CRL Issuance Frequency (If Applicable)	57
4.4.10	Certificate Revocation List Checking Requirements.....	57
4.4.11	On-Line Revocation/Status Checking Availability	57
4.4.12	On-Line Revocation Checking Requirements	58
4.4.13	Other Forms of Revocation Advertisements Available.....	58
4.4.14	Checking Requirements for Other Forms of Revocation Advertisements	58
4.4.15	Special Requirements Regarding Key Compromise.....	58
4.5	Security Audit Procedures	58
4.5.1	Types of Events Recorded	58
4.5.1.1	Events Recorded by Processing Centers (Class 1-3)	58
4.5.1.2	Events Recorded by Service Centers, Managed PKI Customers (Class 1-3)..	59
4.5.1.3	Events Recorded by Gateway Customers (Class 1).....	59
4.5.2	Frequency of Processing Log (Class 1-3).....	60
4.5.3	Retention Period for Audit Log (Class 1-3).....	60
4.5.4	Protection of Audit Log (Class 1-3).....	60
4.5.5	Audit Log Backup Procedures (Class 1-3)	60
4.5.6	Audit Collection System (Class 1-3)	60
4.5.7	Notification to Event-Causing Subject (Class 1-3).....	60
4.5.8	Vulnerability Assessments (Class 1-3)	61
4.6	Records Archival (Class 1-3).....	61
4.6.1	Types of Events Recorded	61
4.6.2	Retention Period for Archive	61
4.6.3	Protection of Archive.....	61
4.6.4	Archive Backup Procedures.....	62

4.6.5	Requirements for Time-Stamping of Records	62
4.6.6	Archive Collection System	62
4.6.7	Procedures to Obtain and Verify Archive Information.....	62
4.7	Key Changeover (Renewal) (Class 1-3)	62
4.8	Compromise and Disaster Recovery (Class 1-3).....	63
4.8.1	Computing Resources, Software, and/or Data Are Corrupted.....	63
4.8.2	Entity Public Key is Revoked.....	63
4.8.3	Entity Key is Compromised.....	63
4.8.4	Secure Facility After a Natural or Other Type of Disaster	63
4.9	CA Termination (Class 1-3).....	64
5.	Physical, Procedural, and Personnel Security Controls	65
5.1	Physical Controls	65
5.1.1	Site Location and Construction.....	65
5.1.1.1	Gateway Customer Requirements (Class 1)	65
5.1.1.2	Managed PKI Customer Requirements (Class 1-3).....	65
5.1.1.3	Service Center Requirements (Class 1-3).....	65
5.1.1.4	Processing Center Requirements (Class 1-3).....	66
5.1.2	Physical Access.....	66
5.1.2.1	Requirements for Gateway Customers (Class 1) and Managed PKI Customers (Class 1-3).....	66
5.1.2.2	Service Center Requirements (Class 1-3).....	67
5.1.2.3	Processing Center Requirements (Class 1-3).....	67
5.1.3	Power and Air Conditioning (Class 1-3)	67
5.1.4	Water Exposures (Class 1-3)	67
5.1.5	Fire Prevention and Protection (Class 1-3).....	67
5.1.6	Media Storage (Class 1-3)	67
5.1.7	Waste Disposal (Class 1-3).....	67
5.1.8	Off-Site Backup (Class 1-3).....	68
5.2	Procedural Controls	68
5.2.1	Trusted Roles	68
5.2.1.1	Gateway Customer (Class 1) and Processing Center (Class 1-3) Trusted Roles 68	
5.2.1.2	Service Center and Managed PKI Customer (Class 1-3) Trusted Roles	68
5.2.1.3	ASB Customer (Class 2-3) Trusted Roles	69
5.2.2	Number of Persons Required Per Task (Class 1-3)	69
5.2.3	Identification and Authentication for Each Role (Class 1-3).....	69
5.3	Personnel Controls	69
5.3.1	Background, Qualifications, Experience, and Clearance Requirements (Class 1-3) 69	
5.3.2	Background Check Procedures	70
5.3.2.1	Background Check Procedures for Gateway Customers (Class 1), ASB Customers (Class 2-3), and Managed PKI Customers (Class 1-3).....	70
5.3.2.2	Background Check Procedures for Service Centers and Processing Centers (Class 1-3).....	71
5.3.3	Training Requirements (Class 1-3).....	71
5.3.4	Retraining Frequency and Requirements (Class 1-3)	71

5.3.5	Job Rotation Frequency and Sequence (Class 1-3)	71
5.3.6	Sanctions for Unauthorized Actions (Class 1-3)	71
5.3.7	Contracting Personnel Requirements (Class 1-3)	72
5.3.8	Documentation Supplied to Personnel (Class 1-3)	72
6.	Technical Security Controls	72
6.1	Key Pair Generation and Installation	72
6.1.1	Key Pair Generation (Class 1-3)	72
6.1.2	Private Key Delivery to Entity (Class 1-3)	72
6.1.3	Public Key Delivery to Certificate Issuer (Class 1-3)	73
6.1.4	CA Public Key Delivery to Users (Class 1-3)	73
6.1.5	Key Sizes (Class 1-3)	73
6.1.6	Public Key Parameters Generation (Class 1-3)	74
6.1.7	Parameter Quality Checking (Class 1-3)	74
6.1.8	Hardware/Software Key Generation (Class 1-3)	74
6.1.9	Key Usage Purposes (As per X.509 v3 Key Usage Field) (Class 1-3)	74
6.2	Private Key Protection	75
6.2.1	Standards for Cryptographic Modules (Class 1-3)	75
6.2.2	Private Key (m out of n) Multi-Person Control (Class 1-3)	76
6.2.3	Private Key Escrow (Class 1-3)	76
6.2.4	Private Key Backup (Class 1-3)	77
6.2.5	Private Key Archival (Class 1-3)	77
6.2.6	Private Key Entry into Cryptographic Module (Class 1-3)	77
6.2.7	Method of Activating Private Key	78
6.2.7.1	End-User Subscriber Private Keys	78
6.2.7.1.1	Class 1 Certificates	78
6.2.7.1.2	Class 2 Certificates	78
6.2.7.1.3	Class 3 Certificates Other Than Administrator Certificates	78
6.2.7.2	Administrators' Private Keys (Class 3)	79
6.2.7.2.1	Administrators	79
6.2.7.2.2	Managed PKI Administrators using a Cryptographic Module (with Automated Administration or with Managed PKI Key Manager Service)	79
6.2.7.3	Gateway Customers' Private Keys (Class 1)	79
6.2.7.4	Private Keys Held by Processing Centers (Class 1-3)	80
6.2.8	Method of Deactivating Private Key	80
6.2.8.1	End-User Subscribers	80
6.2.8.1.1	Class 1 Certificates	80
6.2.8.1.2	Class 2 Certificates	80
6.2.8.1.3	Class 3 Certificates	80
6.2.8.2	Gateway Customers (Class 1)	80
6.2.8.3	Processing Centers (Class 1-3)	80
6.2.9	Method of Destroying Private Key	81
6.2.9.1	Gateway Customers (Class 1)	81
6.2.9.2	Processing Centers (Class 1-3)	81
6.3	Other Aspects of Key Pair Management (Class 1-3)	81
6.3.1	Public Key Archival	81
6.3.2	Usage Periods for the Public and Private Keys	81

6.4	Activation Data	82
6.4.1	Activation Data Generation and Installation	82
6.4.1.1	End-User Subscribers (Class 1-3)	82
6.4.1.2	Administrators (Class 3)	83
6.4.1.3	Gateway Customers (Class 1)	83
6.4.1.4	Processing Centers (Class 1-3)	83
6.4.2	Activation Data Protection	83
6.4.2.1	End-User Subscribers (Class 1-3) and Gateway Customers (Class 1)	83
6.4.2.2	Processing Centers (Class 1-3)	83
6.4.3	Other Aspects of Activation Data (Class 1-3)	84
6.4.3.1	Activation Data Transmission	84
6.4.3.2	Activation Data Destruction	84
6.5	Computer Security Controls	84
6.5.1	Specific Computer Security Technical Requirements	84
6.5.1.1	Controls for Processing Centers (Class 1-3)	84
6.5.1.2	Controls for Gateway Customers (Class 1)	85
6.5.1.3	Controls for Service Centers and Managed PKI Customers (Class 1-3)	85
6.5.2	Computer Security Rating (Class 1-3)	85
6.6	Life Cycle Technical Controls (Class 1-3)	85
6.6.1	System Development Controls	85
6.6.1.1	Software Used by Gateway Customers	85
6.6.1.2	Software Used by Managed PKI Customers, Service Centers, and Processing Centers	86
6.6.2	Security Management Controls	86
6.6.2.1	Software Used by Gateway Class 1 Customers	86
6.6.2.2	Software Used by Managed PKI Customers, Service Centers, and Processing Centers	86
6.6.3	Life Cycle Security Ratings	86
6.7	Network Security Controls (Class 1-3)	86
6.8	Cryptographic Module Engineering Controls (Class 1-3)	87
7.	Certificate and CRL Profile (Class 1-3)	87
7.1	Certificate Profile	87
7.1.1	Version Number(s)	87
7.1.2	Certificate Extensions	88
7.1.2.1	Key Usage	88
7.1.2.2	Certificate Policies Extension	88
7.1.2.3	Subject Alternative Names	88
7.1.2.4	Basic Constraints	88
7.1.2.5	Extended Key Usage	89
7.1.2.6	CRL Distribution Points	89
7.1.2.7	Authority Key Identifier	89
7.1.2.8	Subject Key Identifier	89
7.1.3	Algorithm Object Identifiers	90
7.1.4	Name Forms	90
7.1.5	Name Constraints	90
7.1.6	Certificate Policy Object Identifier	90

7.1.7	Usage of Policy Constraints Extension.....	90
7.1.8	Policy Qualifiers Syntax and Semantics.....	91
7.1.9	Processing Semantics for the Critical Certificate Policy Extension.....	91
7.2	CRL Profile.....	91
7.2.1	Version Number(s).....	91
7.2.2	CRL and CRL Entry Extensions.....	91
8.	Specification Administration (Class 1-3)	91
8.1	Specification Change Procedures.....	91
8.1.1	Items that Can Change Without Notification.....	91
8.1.2	Items that Can Change with Notification.....	91
8.1.2.1	List of Items.....	92
8.1.2.2	Notification Mechanism.....	92
8.1.2.3	Comment Period.....	92
8.1.2.4	Mechanism to Handle Comments.....	92
8.1.3	Changes Requiring Changes in the Certificate Policy OID or CPS Pointer.....	92
8.2	Publication and Notification Policies.....	93
8.2.1	Items Not Published in the CP.....	93
8.2.2	Distribution of the CP.....	93
8.3	CPS Approval Procedures.....	93
	Acronyms and Definitions	93
	Table of Acronyms.....	93
	Definitions.....	94

1. Introduction

VeriSign, Inc. (“VeriSign”) is the leading provider of trusted infrastructure services to web sites, enterprises, electronic commerce service providers, and individuals. The company’s domain name, digital certificate, and payment services provide the critical web identity, authentication, and transaction infrastructure that online businesses require to conduct secure e-commerce and communications.

Please Note: The capitalized terms in this CP are defined terms with specific meanings. Please see Section 9 for a list of definitions.

VeriSign provides digital certificates (“Certificates”) for both wired and wireless applications through a global public key infrastructure (“PKI”) known as the VeriSign Trust NetworkSM (“VTN”), as well as on a private label basis. VeriSign designed the VTN to accommodate a large, public, and widely distributed community of users with diverse needs for communications and information security. VeriSign offers VTN services together with a global network of affiliates (“Affiliates”) throughout the world.

This document, called the “CP,” is entitled “The VeriSign Trust Network Certificate Policies.” The CP is the principal statement of policy governing the VTN. The CP sets forth the business, legal, and technical requirements for approving, issuing, managing, using, revoking, and renewing, digital Certificates within the VTN and providing associated trust services. These requirements, called the “VTN Standards,” protect the security and integrity of the VTN. VTN Standards comprise a single set of rules that apply consistently VTN-wide, thereby providing assurances of uniform trust throughout the VTN.

The VTN includes three classes of Certificates, Classes 1-3. The CP describes how these three Classes correspond to three classes of applications with common security requirements. The CP is a single document that defines three certificate policies, one for each of the Classes. The current version of the CP identifies the VTN Standards applicable to each Class.

The authors of this document comprise the members of the VeriSign Trust Network Policy Management Authority (“PMA”). The PMA is responsible for proposing changes to the CP, updating the document, and soliciting comments on the CP. The PMA also oversees compliance with the requirements of this CP.

1.1 Overview

The CP establishes requirements for the entire VTN, but only the VTN. The CP governs the use of the VTN by all individuals and entities within the VTN (collectively, “VTN Participants”). Moreover, VeriSign and all Affiliates worldwide must follow the requirements of the CP. VeriSign and each Affiliate has authority over a portion of the VTN. The portion of the VTN controlled by VeriSign or an Affiliate is called its “Subdomain” of the VTN. An Affiliate’s Subdomain consists of the portion of the VTN under its control. An Affiliate’s Subdomain includes entities subordinate to it such as its Customers, Subscribers, and Relying Parties. Nonetheless, the CP acts as an umbrella document establishing baseline VTN Standards for the entire VTN.

The CP, however, does not govern any services outside the VTN. For example, VeriSign and certain Affiliates offer private label services by which organizations create their own private hierarchies outside the VTN, approve certificate applications, and outsource to VeriSign or an Affiliate the back-end functions of certificate issuance, management, revocation, and renewal. Because the CP applies only to the VTN, it does not apply to these private hierarchies.

(a) Role of the VTN CP and Other Practices Documents

The CP describes at a general level the overall business, legal, and technical infrastructure of the VTN. More specifically, it describes, among other things:

- Appropriate applications for, and the assurance levels associated with, each class of Certificate,
- Obligations of Certification Authorities, Registration Authorities, Subscribers, and Relying Parties,
- Legal matters that must be covered in VTN Subscriber Agreements and Relying Party Agreements,
- Requirements for audit and related security and practices reviews,
- Methods to confirm the identity of Certificate Applicants for each Class of Certificate,
- Operational procedures for Certificate lifecycle services: Certificate Applications, issuance, acceptance, revocation, and renewal,
- Operational security procedures for audit logging, records retention, and disaster recovery,
- Physical, personnel, key management, and logical security,
- Certificate and Certificate Revocation List content, and
- Administration of the CP, including methods of amending it.

The CP, however, is only the first in a set of documents relevant to the VTN. These other documents include:

- Ancillary security and operational documents that supplement the CP by providing more detailed requirements, such as:
 - The VeriSign Physical Security Policy, which sets forth security principles governing VTN infrastructure,
 - The Security and Audit Requirements Guide, which describes detailed requirements for VeriSign and Affiliates concerning personnel, physical, telecommunications, logical, and cryptographic key management security,
 - ,
 - Affiliate Practices Legal Requirements Guidebook, which places requirements on Affiliates to draft a set of practice and legal documents that are in an acceptable local language, comply with local law, and reflect certain localized procedures, and to draft a privacy policy and validation plan describing how Affiliates will authenticate individuals and organizations for each class and type of Certificates they plan to offer, and
 - Key Ceremony Reference Guide, which presents detailed key management operational requirements.

- “Certification Practice Statements.” VeriSign and each Affiliate will have a CPS. While the CP sets forth requirements (VTN Standards), a CPS explains how VeriSign or the Affiliate employs practices and procedures to meet those requirements.
- Ancillary agreements imposed by VeriSign or an Affiliate. These agreements would bind Customers, Subscribers, and Relying Parties of VeriSign or an Affiliate. Among other things, the agreements flow down VTN Standards to these VTN Participants and, in some cases, state specific practices for how they must meet VTN Standards.

In many instances, the CP refers to these ancillary documents for specific, detailed VTN Standards where including the specifics in the CP would compromise VTN security. Figure 1 shows the relationship between the CP and other practices documents.

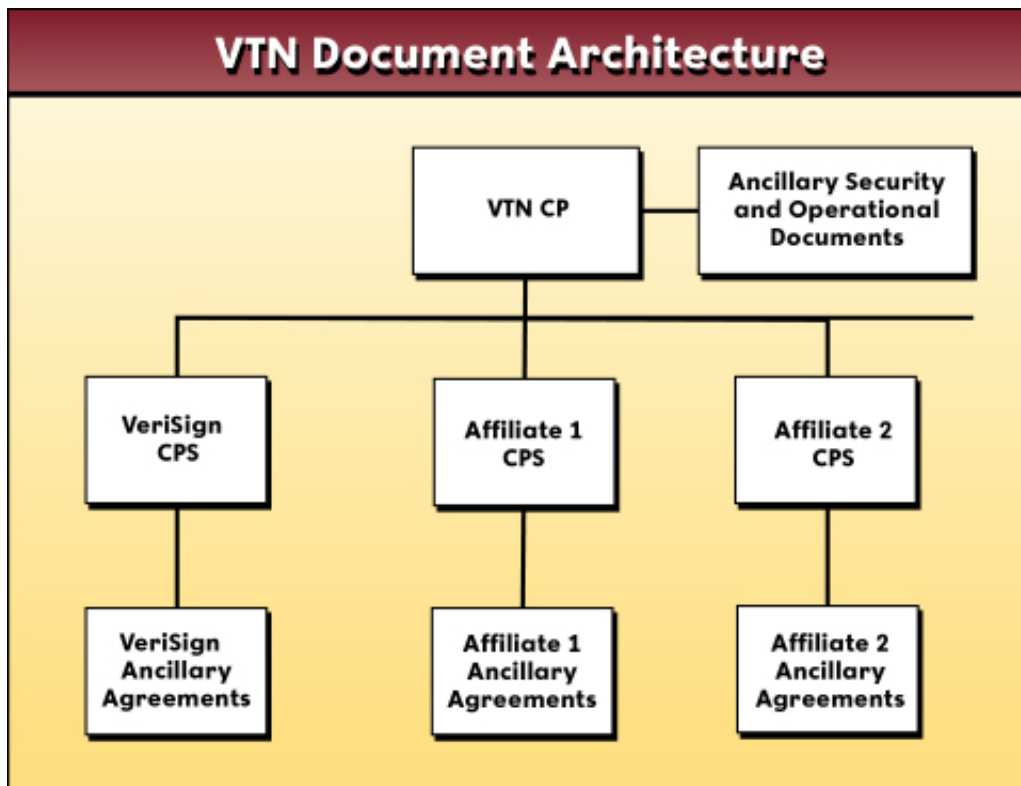


Figure 1 - VTN Document Architecture

As shown in Figure 1, the CP is at the apex of the VTN document architecture and sets high-level VTN Standards. Ancillary security and operational documents supplement the CP in setting more detailed VTN Standards. VeriSign and each Affiliate have a CPS describing how VTN Standards are met. Finally, VeriSign and each Affiliate use ancillary agreements and documents to place requirements on VTN Participants.

VeriSign and the PMA maintain the CP and the VTN ancillary security and operational documents. By contrast, VeriSign and each Affiliate maintain their own CPSs and ancillary agreements. Each Affiliate must draft and maintain a CPS and a set of ancillary agreements as a condition of beginning and continuing operations as an Affiliate within the VTN. These documents must be reviewed and approved by the PMA.

Table 1 is a matrix showing various VTN practices documents, whether they are publicly available, and their locations. The list in Table 1 is not intended to be exhaustive. Note that documents not expressly made public are confidential to preserve the security of the VTN.

<i>Documents</i>	<i>Status</i>	<i>Where Available to the Public</i>
VeriSign Trust Network Certificate Policies	Public	VeriSign Repository per CP § 8.2.2. See https://www.verisign.com/repository
<i>VTN Ancillary Security and Operational Documents</i>		
VeriSign Information Security Policy	Confidential	N/A
VeriSign Physical Security Policy	Confidential	N/A
Security and Audit Requirements Guide	Confidential	N/A
Key Ceremony Reference Guide	Confidential	N/A
Affiliate Practices Legal Requirements Guidebook	Confidential	N/A
Affiliate Audit Program Guide	Confidential	N/A
Managed PKI Administrator's Handbook	Public	https://www.verisign.com/enterprise/library/index.html
Managed PKI Key Management Service Administrator's Guide	Public	https://www.verisign.com/enterprise/library/index.html
<i>VeriSign- or Affiliate-Specific Documents</i>		
VeriSign Certification Practice Statement	Public	VeriSign Repository per CP § 2.6.1. See https://www.verisign.com/repository
Affiliates' CPSs	Public	Affiliates' repositories per CP § 2.6.1. See repository sections of Affiliates' web sites.
VeriSign's ancillary agreements (Managed PKI Agreements, Subscriber Agreements, and Relying Party Agreements)	Public, including Managed PKI Lite agreements, but not Managed PKI agreements, which are confidential	VeriSign Repository per CP § 2.6.1. See https://www.verisign.com/repository
Affiliates' ancillary agreements	Form web-based agreements are public, but agreements with enterprise Customers are not.	Affiliates' repositories per CP § 2.6.1. See repository sections of Affiliates' web sites.

Table 1 – Availability of Practices Documents

(b) Background Concerning Digital Certificates and the VTN Hierarchy

This CP assumes that the reader is generally familiar with Digital Signatures, PKIs, and VeriSign's VTN. If not, VeriSign advises that the reader obtain some training in the use of public key cryptography and public key infrastructure as implemented in the VTN. Educational

and training information is accessible from VeriSign at <http://www.verisign.com>. Additional assistance is available from VeriSign customer service representatives (customer_service@verisign.com). Finally, the following is a brief summary of the roles of the different VTN Participants.

At the heart of the VTN is a hierarchy of entities called “Certification Authorities” or “CAs.” CAs act as trusted third parties to facilitate the confirmation of the binding between a public key and the identity and/or other attributes of the individual, entity, or device that is the “Subject” of the Certificate. (Subjects of Certificates are the same as Subscribers, except in the case of devices, where the Subscriber is the party that owns the device and that has been issued a Certificate.)

“CA” is an umbrella term that refers to entities that issue Certificates to end-user Subscribers or other CAs above them in the hierarchy. One subcategory of CA is the Primary Certification Authority (“PCA”). PCAs act as roots in the VTN, and one PCA corresponds to each Class of Certificate. A CA may be a VeriSign CA, which means it is owned and operated by VeriSign. For example, all PCAs are VeriSign CAs. Other CAs are non-VeriSign entities, such as the CAs of Affiliates and certain Customers.

CAs sometimes delegate identity confirmation functions to one or more “Registration Authorities” or “RAs.” RAs establish enrollment procedures on behalf of a CA, obtain Certificate Applications, confirm the identity of Certificate Applicants, and either approve or deny Certificate Applications. RAs can also initiate Certificate revocation, upon the request of a Subscriber or otherwise, although the CA itself actually carries out the revocation by including the Certificate in a Certificate revocation list (“CRL”) or otherwise indicating that a Certificate has been revoked in the CA’s repository.

Subscribers are individuals or organizations that obtain Certificates for use in their applications. For example, individuals can use a Certificate to send another party a digitally signed e-mail. An organization may use a Certificate, for instance, on a server to create a secure session with web browser using Secure Sockets Layer (“SSL”). SSL creates a secure channel between a web browser and web server. SSL authenticates the server to the client, provides message integrity, and encrypts communication between the server and client.

Relying parties are individuals or organizations that use the Certificates of others for a particular application. For instance, the recipient of a digitally signed e-mail can use the sender’s Certificate to verify the digital signature on the message. In addition, the sender of an encrypted e-mail can use the recipient’s Certificate to encrypt a key that in turn is used to encrypt the message. Only the recipient having the private key corresponding to the public key in the Certificate can obtain the key so as to decrypt the message.

Before a Subscriber obtains a Certificate, the Subscriber must first enroll for a Certificate as a Certificate Applicant. Certificate Applicants must complete the enrollment process established by a CA or RA, in which a Certificate Application is submitted to the CA or RA. In response to a Certificate Application, the CA or RA confirms the identity and/or other attributes of the

Certificate Applicant and either approves or denies the Certificate Application. If the Certificate Application is approved, a Certificate is issued to the Certificate Applicant.

Following issuance, the CA makes the Certificate available to the Certificate Applicant. In most cases, a Certificate Applicant retrieves a client Certificate by accessing a specified web page that loads the Certificate into the Certificate Applicant's software. Alternatively, the Certificate may be delivered to the Certificate Applicant, which the Certificate Applicant loads into its software. Such retrieval and/or loading of a Certificate into software constitutes acceptance of the Certificate, at which time the Certificate Applicant becomes a Subscriber, unless the Subscriber previously manifested acceptance. The Subscriber must review the Certificate and notify the CA or RA of any mistakes in the Certificate content after receiving access to the Certificate. The new Subscriber agrees to be bound by Subscribers' obligations through a Subscriber Agreement.

(c) Compliance with Applicable Standards

The structure of this CP generally corresponds to the *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*, known as RFC 2527 of the Internet Engineering Task Force, an Internet standards body. This document serves to define three "certificate policies," within the meaning of RFC 2527. The RFC 2527 framework has become a standard in the PKI industry. This CP conforms to the RFC 2527 framework in order to make policy mapping and comparisons, assessment, and interoperation easier for persons using or considering using VTN services.

VeriSign has conformed the CP to the RFC 2527 structure where possible, although slight variances in title and detail are necessary because of the complexity of VTN business models. While VeriSign intends to continue the policy of adhering to RFC 2527 in the future, VeriSign reserves the right to vary from the RFC 2527 structure as needed, for example to enhance the quality of the CP or its suitability to the VTN. Moreover, the CP's structure may not correspond to future versions of RFC 2527.

(d) Interoperation with Other PKIs

VeriSign will consider interoperation with other PKIs on a case-by-case basis. The PMA is responsible for approving or rejecting any requests for such interoperation. This interoperation includes, but is not limited to, specific types of cross-certification. Cross-certification may include issuing cross-Certificates or being issued cross-Certificates. VeriSign will consider interoperation with a hierarchy for a specific class of Certificates by evaluating factors that include, but are not limited to:

- The degree to which the non-VTN PKI provides a substantially similar function and level of assurance and trustworthiness in comparison with VTN services for that Class of Certificates,
- The degree to which interoperation would enhance the value of VTN services to Affiliates, Customers, Subscribers, and Relying Parties,
- The ability for the interoperating PKIs to support the comprehensive set of robust lifecycle services in a seamless fashion, and
- The relative business need for such interoperation.

Any such interoperation would require the execution of an appropriate interoperation agreement.

1.1.1 Policy Overview

VeriSign offers three distinct classes of certification services, Classes 1-3, for both the wired and wireless Internet and other networks. Each level, or class, of Certificate provides specific functionality and security features and corresponds to a specific level of trust. VTN Participants choose which Classes of Certificates they need. As VeriSign observes new patterns of usage and market demand, it will consider providing new Classes or types of Certificates.

Class 1 Certificates, issued only to individuals, provide the lowest level of assurances within the VTN. They provide assurances that the Subscriber's distinguished name is unique and unambiguous within VeriSign's or an Affiliate's Subdomain and that a certain e-mail address is associated with a public key. They are appropriate for digital signatures, encryption, and access control for non-commercial or low-value transactions where proof of identity is unnecessary.

Class 2 Certificates, also issued only to individuals, provide a medium level of assurances within the VTN. They provide assurances of the identity of the Subscriber based on a comparison of information submitted by the Certificate applicant against information in business records or databases or the database of a VeriSign-approved identity proofing service. They can be used for digital signatures, encryption, and access control, including as proof of identity in medium-value transactions.

Class 3 Certificates provide the highest level of assurances within the VTN. Class 3 Certificates are issued to individuals, organizations, and Administrators for CAs and RAs. Class 3 individual Certificates may be used for digital signatures, encryption, and access control, including as proof of identity, in high-value transactions. Class 3 individual Certificates provide assurances of the identity of the Subscriber based on the personal (physical) presence of the Subscriber before a person that confirms the identity of the Subscriber using a well-recognized form of government-issued identification and one other identification credential. Other Class 3 organizational Certificates are issued to devices to provide authentication; message, software, and content integrity; and confidentiality encryption. Class 3 organizational Certificates provide assurances of the identity of the Subscriber based on a confirmation that the Subscriber organization does in fact exist, that the organization has authorized the Certificate Application, and that the person submitting the Certificate Application on behalf of the Subscriber was authorized to do so.

“Class 3 Organizational ASB Certificates” (*see* CP § 1.1.2.2.1) are issued to an organization for use by a duly authorized representative, who uses the Certificate on behalf of the organization. The representative may use the Certificates for digital signatures, encryption, and access control. Class 3 Organizational ASB Certificates provide an assurance, not only that a public key is bound to a particular organization, but also that the person controlling the organization's private key is authorized to act on behalf of the organization in transactions entered into using the private key corresponding to the public key in the Certificate.

In general, all three classes of VTN Certificates fall within two categories, Retail and Managed PKI . Retail Certificates are Certificates issued by VeriSign or an Affiliate, acting as CA, to individuals or organizations applying one by one to VeriSign or an Affiliate on its web site. Managed PKI Certificates are based on a Certificate Application approved by an Managed PKI Customer that enters into an Managed PKI Agreement with either VeriSign or an Affiliate for the issuance of a certain quantity of Certificates (*see* CP § 1.1.2.1.1).

In addition to Retail and Managed PKI Certificates, VTN Certificates are issued by Gateway Customers, for Administrators of CAs and RAs, and through the Authentication Service Bureau. Gateway Customers are CAs using Certificate server software of Microsoft and Netscape that have been included within the VTN by virtue of a Certificate issued to the Gateway Customer from VeriSign. Gateway Customers use their Certificate servers to issue Certificates to Subscribers. For more information about Gateway, see CP § 1.1.2.1.5. Administrator Certificates are issued to CA or RA Administrators to allow them to perform administrative functions on behalf of the CA or RA. Under the Authentication Service Bureau program, VeriSign or an Affiliate confirms the identity of a Certificate Applicant on behalf of an organization, such as a business-to-business (B2B) exchange. For more information about Authentication Service Bureau, see CP § 1.1.2.2.1.

Table 2 sets forth the properties of each Certificate class, based on whether they are issued to individuals or organizations, and whether they are offered on a Retail or Managed PKI basis, offered through the Gateway or Authentication Service Bureau program, or issued to Administrators.

<i>Class</i>	<i>Issued to</i>	<i>Services Under Which Certificates are Available</i>	<i>Confirmation of Certificate Applicants' Identity (CP §§ 3.1.8.1, 3.1.9)</i>	<i>Applications implemented or contemplated by Users (CP § 1.3.4.1)</i>
<i>Class 1</i>	Individuals	Retail	Name and e-mail address search to ensure that the distinguished name is unique and unambiguous.	Modestly enhancing the security of e-mail through confidentiality encryption, digital signatures, and web-based access control, where proof of identity is unnecessary. Applications requiring a low level of assurances in comparison with the other Classes, such as non-commercial web browsing and e-mail.
		Managed PKI and Gateway	Name and e-mail address search as with Class 1 Retail plus checking internal documentation or databases to confirm the Certificate Applicant's affiliation with the managed PKI Customer or Gateway Customer as an Affiliated Individual.	
<i>Class 2</i>	Individuals	Retail and Authentication Service Bureau	Same as Class 1 Retail, plus automated or out-of-band enrollment information check with one or more third-party databases or comparable sources.	Enhancing the security of e-mail through confidentiality encryption, digital signatures for authentication, and web based access control. Applications

Class	Issued to	Services Under Which Certificates are Available	Confirmation of Certificate Applicants' Identity (CP §§ 3.1.8.1, 3.1.9)	Applications implemented or contemplated by Users (CP § 1.3.4.1)
		Managed PKI	Same as Class 1 Retail plus checking internal documentation or databases to confirm identity of the Certificate Applicant (e.g., human resources documentation) and that the Certificate Applicant is affiliated with the Managed PKI Customer.	requiring a medium level of assurances in comparison with the other Classes, such as some individual and intra- and inter-company e-mail, on-line subscriptions, account applications, and password replacement.
Class 3	Individuals	Retail	Same as Class 1 Retail, plus personal presence and check of one or more ID credentials.	Enhancing the security of e-mail through confidentiality encryption, digital signatures for authentication, and web based access control. Applications requiring a high level of assurances in comparison with the other Classes, such as some online banking, corporate database access, and exchanging confidential information.
		Administrators	Specialized confirmation procedures depending upon the type of Administrator. The identity of the Administrator and the organization utilizing the Administrator are confirmed. <i>See also CP § 5.2.3.</i>	Administrator functions.
	Organizations	Retail	Check of third-party database or other documentation showing proof of right to use the organizational name. Validation check by telephone (or comparable procedure) to confirm information in, and authorization of, the Certificate Application. In the case of web server Certificates, confirmation that the Certificate Applicant has the right to use the domain name to be placed in the Certificate.	Server authentication, (some examples being web, ftp, or directory authentication), secure SSL/TLS sessions, confidentiality encryption, and (when communicating with other servers) client authentication (Secure Server ID, Global Server ID, OFX, and authentication and integrity of software and other content (Code and Content Signing Digital IDs).

<i>Class</i>	<i>Issued to</i>	<i>Services Under Which Certificates are Available</i>	<i>Confirmation of Certificate Applicants' Identity (CP §§ 3.1.8.1, 3.1.9)</i>	<i>Applications implemented or contemplated by Users (CP § 1.3.4.1)</i>
		Authentication Service Bureau	Check of third-party database or other documentation showing the existence of the organization. Validation check by telephone (or comparable procedure) to organization to confirm employment and authority of organizational representative, and to the representative to confirm his or her Certificate Application. Letter confirming the Certificate Application is sent to the representative.	Enhancing the security of e-mail sent on behalf of an organization through confidentiality encryption, digital signatures for authentication, and web based access control. Applications requiring a high level of assurances in comparison with the other Classes, such as gaining access to a B2B extranet or conducting high-value transactions on a B2B exchange.
		Managed PKI	Validation of Managed PKI for SSL Customer or Managed PKI for SSL Premium Edition Customer as in Class 3 organizational Retail, plus validation of Managed PKI Administrator.	Server authentication, confidentiality encryption, and (when communicating with other properly enabled servers) client authentication (Secure Server ID and Global Server ID).

Table 2 - Certificate Properties Affecting Trust

The specifications for Classes of Certificates in this CP set forth the minimum level of assurances provided for each Class. For example, any Class 1 Certificate may be used for digital signatures, encryption, and access control where proof of identity is not necessary, that is, for applications requiring a low level of assurances. Nonetheless, by contract or within specific environments (such as an intra-company environment), VTN Participants are permitted to use validation procedures stronger than the ones set forth within the CP, or use Certificates for higher security applications than the ones described in CP §§ 1.1.1, 1.3.4.1. Any such usage, however, shall be limited to such entities and subject to CP §§ 2.2.1.2, 2.2.2.2, and these entities shall be solely responsible for any harm or liability caused by such usage.

1.1.2 VTN Suite of Services

The VTN offers a series of services to assist in the deployment, management, and uses of Certificates. This section provides a general description of each of these services. For more information about any of these programs, consult VeriSign's web site at <http://www.verisign.com>. All of such services are subject to the specific agreements with VeriSign or the Affiliate providing them.

1.1.2.1 Certificate Distribution Services

1.1.2.1.1 VeriSign Managed PKI

VeriSign Managed PKI is a fully integrated managed PKI service that allows enterprise Customers of VeriSign and its Affiliates to provide Certificates to individuals, such as employees, partners, suppliers, and customers, as well as devices, such as servers, routers, and

firewalls. Managed PKI permits enterprises to secure messaging, intranet, extranet, virtual private network, and e-commerce applications. Using Managed PKI, an enterprise can perform Certificate lifecycle management and exploit the high-availability Certificate processing services of VeriSign and its Affiliates, without assuming the burden of designing, provisioning, staffing, and maintaining its own PKI. VeriSign has extended the VeriSign Managed PKI services with Go Secure!SM, a suite of plug-and-play services designed to accelerate the way enterprises deploy secure e-commerce applications, including e-mail and browsing applications, directories, VPN devices, web servers, and enterprise resource planning solutions.

Managed PKI is, at its heart, an outsourcing service. Customers of VeriSign or its Affiliates obtaining VeriSign Managed PKI (“Managed PKI Customers”) fall into three categories. First, some Managed PKI Customers (“Managed PKI Managed PKI Customers”) provide client Certificates by becoming a Certification Authority within the VTN. Managed PKI Managed PKI Customers perform the RA “front-end” functions of approving or denying Certificate Applications, and initiating the revocation or renewal of Certificates using Managed PKI functionality. RA functions are a subset of CA functions. At the same time, the Managed PKI Managed PKI Customer can leverage the secure PKI backbone of the VeriSign Trust Network by outsourcing all “back-end” Certificate issuing, management, revocation, and renewal functions to VeriSign or an Affiliate. (For a discussion of Affiliates and Processing Centers, see CP § 1.1.2.1.2.)

The second category of Managed PKI Customers (“Managed PKI Managed PKI Lite Customers”) uses Managed PKI Lite, which provides security for smaller enterprises and organizations than typical Managed PKI Customers. Managed PKI Lite Customers become Registration Authorities associated with a VeriSign or Affiliate CA, which is shared among VeriSign’s or an Affiliate’s Managed PKI Lite Customers of the specific class of Certificates. Managed PKI Lite Customers, like Managed PKI Customers, approve or deny Certificate Applications using Managed PKI functionality, and request the revocation or renewal of Certificates. As with Managed PKI Customers, VeriSign or another Processing Center performs all the back-end Certificate issuance, management, revocation, and renewal functions, as with Managed PKI Customers.

The final categories of Managed PKI Customers approve Certificate Applications for server Certificates known as Secure Server IDs (“Managed PKI for SSL Customers”) and for server Certificates known as Global Server IDs (“Global Server Managed PKI Customers”). (For a discussion of the differences between Secure Server IDs and Global Server IDs, see CP § 1.3.4.1.3.2.) Managed PKI for SSL Customers and Managed PKI for SSL Premium Edition Customers become Registration Authorities associated with a VeriSign CA, which is shared among all VTN Managed PKI for SSL Customers or Managed PKI for SSL Premium Edition Customers. Managed PKI for SSL Customers and Managed PKI for SSL Premium Edition Customers, as with other Managed PKI Customers, approve or deny Certificate Applications using Managed PKI functionality, and request the revocation or renewal of Certificates. Moreover, as with other Managed PKI Certificates, VeriSign performs all the back-end Certificate issuance, management, revocation, and renewal functions.

Managed PKI Customers and Managed PKI Lite Customers are not permitted to approve the Certificate Applications of anyone other than one of their own Affiliated Individuals, except as

noted below. Managed PKI Customers may not approve Certificate Applications for VTN Certificates issued to the general public. The Authentication Service Bureau, however, provides one solution for organizations seeking to obtain Certificates for unaffiliated individuals and organizational representatives. *See CP § 1.1.2.2.1.*

In addition, VeriSign offers a service to widen the scope of affiliation permitted under Managed PKI, called the “Two-Tier Authentication Service.” Managed PKI Customers may wish to obtain Certificates for a certain user base that they do not know themselves, but is known by the organizations with which they transact. For example, a manufacturer Managed PKI Customer may wish to distribute Certificates, not to its own employees, but to the employees of the retailing companies distributing its products. The employees are known to the retailers, but not to the manufacturer itself. The Two-Tier Authentication Service would permit the manufacturer to distribute Certificates to the employees of these retailers.

Specifically, the Two-Tier Authentication Service permits a Managed PKI Customer, like the manufacturer in this example, to delegate RA functions to organizations with which it has a relationship, like the retailers in the example. These organizations must enter into an agreement, approved by VeriSign or an Affiliate, confirming this delegation and requiring them to perform RA obligations. Certificate Applicants must be Affiliated Individuals in relation to these organizations.

A Managed PKI for SSL Customer or Managed PKI for SSL Premium Edition Customer may only approve Certificate Applications for servers within their own organizations. Managed PKI for SSL Customers and Managed PKI for SSL Premium Edition Customers are not permitted to approve the Class 3 Certificate Applications of any servers outside their respective organizations, and may not issue Certificates to the general public.

1.1.2.1.2 VeriSign Affiliate Program

The VTN extends VeriSign’s PKI and certification services globally. VeriSign has partnered with leading e-commerce providers around the world to offer Customers localized service and support. These providers, VeriSign’s Affiliates, act as trusted third parties within the VTN, making the VTN a globally interoperable trust network comprised of a system of providers of certification services that are distributed worldwide. VeriSign’s Affiliates are leaders in the technology, telecommunications, and financial services industries within their local countries or territories. Affiliates add computing infrastructure, expertise in telecommunications, 24x7 data and customer support centers, systems integration, and secure transaction processing to VeriSign’s Certificate issuance technology to become CAs and RAs within the VTN.

Affiliates provide local VTN presence in their respective countries or territories. They market VTN services within their countries or territories. In addition, Affiliates obtain Customers and Subscribers, enter into appropriate contracts with various VTN Participants, and provide customer support to their Customers and Subscribers.

The VeriSign Affiliate Program accommodates two kinds of Affiliates. First, Affiliates can become “Processing Centers,” which create a secure facility housing, among other things, CA systems, including the cryptographic modules holding the private keys used for the issuance of

Certificates. Processing Centers act as CAs in the VTN and perform all Certificate lifecycle services of issuing, managing, revoking, and renewing Certificates. They can also provide lifecycle services on behalf of their Managed PKI Customers or the Managed PKI Customers of the Service Centers subordinate to them.

Second, Affiliates can become “Service Centers,” which do not deploy a facility for back-end Certificate lifecycle services and functions. Rather, Service Centers approve or reject Certificate Applications in the case of Retail Certificates or, in the case of Managed PKI Certificates, arrange with a Processing Center to provide Managed PKI Customers with back-end Certificate lifecycle services. Service Center Affiliates providing client Certificates (“Client Service Centers”) become CAs within the VTN but outsource back-end functions to VeriSign or another Processing Center. When providing server Certificates, however, Service Centers become RAs within the VTN for a VeriSign CA issuing either Secure Server IDs or Global Server IDs. These Service Centers (“Server Service Centers”) perform validation functions to approve or reject Certificate Applications for Secure Server IDs or Global Server IDs. Service Centers can also provide VeriSign Managed PKI services to their Managed PKI Customers. These Managed PKI Customers enter into a Managed PKI agreement with the Service Center, which under its contract with VeriSign or another Processing Center, arranges to have the Processing Center provide back-end Certificate lifecycle services to these Managed PKI Customers.

Affiliates, whether Processing Centers or Service Centers, have the choice of entering into three lines of business, “Consumer,” “Web Site,” and “Enterprise.” “Consumer” refers to Affiliates that provide Class 1, 2 and/or 3 client Retail Certificates on their web sites directly to Certificate Applicants. Processing Centers in the Consumer line of business are CAs, while Service Centers in the Consumer line of business are RAs. “Web Site” refers to Affiliates that provide Secure Server IDs and/or Global Server IDs as Retail Certificates offered directly to organizations applying on the Affiliate’s web site. All Affiliates engaging in the “Web Site” line of business are acting as Service Centers and are RAs for a VeriSign CA, although they may be Processing Centers in one of the other lines of business.

“Enterprise” refers to Affiliates offering VeriSign Managed PKI services to their Customers. These Affiliates, whether a Processing Center or a Service Center, obtain Managed PKI Customers and enter into an appropriate Managed PKI Agreement to perform back-end services for them. The Enterprise line of business is in turn subdivided into Enterprise client and Enterprise server businesses. The Enterprise client business focuses on organizations wishing to obtain client Certificates, who can become Managed PKI Customers or Managed PKI Lite Customers by entering into a Managed PKI Agreement with the Affiliate. If the Affiliate is a Processing Center, the Affiliate performs back-end functions itself for these Managed PKI Customers. By contrast, a Service Center, pursuant to its contract with its Processing Center, arranges to have the Processing Center perform back-end functions for the Service Center’s Managed PKI Customers or Managed PKI Lite Customers.

With regard to the Enterprise server business, organizations wishing to obtain Secure Server IDs or Global Server IDs can become Managed PKI for SSL Customers or Managed PKI for SSL Premium Edition Customers by entering into a Managed PKI Agreement with the Affiliate.

Affiliates in the Enterprise server business are Service Centers, which outsource to VeriSign the obligations of performing Managed PKI services for these Managed PKI Customers.

An Affiliate may have both a Service Center and a Processing Center. For example, an Affiliate may choose to issue Certificates from its secure facility as a Processing Center in the Consumer line of business, but approve Certificate Applications for server Certificates as a Service Center in the Web Site line of business.

1.1.2.1.3 Universal Service Center Program and Other Reseller Programs

VeriSign and Affiliates (with VeriSign's advance written consent) may undertake a program by which they enter into agreements with entities marketing services on their behalf to specific markets ("Resellers"). In addition, VeriSign's Universal Service Center Program permits "Universal Service Centers" to market VeriSign's services to specific markets using a specialized software platform for managing complex, multi-tiered PKI deployment. Universal Service Centers are leading service providers that sell Managed PKI and related services to their Managed PKI Customers and administer the Managed PKI implementations of these Customers using the Universal Service Center Program's software platform. Resellers and Universal Service Centers shall conform to the requirements placed on them by VeriSign and Affiliates through their CPSs, ancillary agreements, and other documents such as guidebooks.

Universal Service Centers do not automatically become CAs themselves. Rather, their Managed PKI Customers become CAs, and it is the function of the Universal Service Center to obtain Customers, enter into appropriate contracts with them, and provide them customer support.

1.1.2.1.4 The Web Host Program

The Web Host Program permits entities acting as a host ("Web Host") to the web sites of their clients to manage lifecycle processes for Retail Secure Server IDs and Global Server IDs on behalf of their clients. A Web Host may be an Internet service provider, a systems integrator, a Reseller, a technical consultant, an application service provider, or similar entity. The Web Host Program offers order management functionality tailored to the Web Host's organization for simplified lifecycle management.

The Web Host Program allows Web Hosts to enroll for Secure Server IDs and Global Server IDs on behalf of end-user Subscribers who are customers of the Web Hosts. Although the Web Host assists the enrollment process (*see* CP § 4.1.1), Web Hosts do not perform validation functions, but instead a Processing Center or Service Center performs these validation functions.

Also, Web Hosts are not themselves the Subscribers of Secure Server IDs and Global Server IDs. Rather, the Web Hosts' customers obtain these Certificates as the actual Subscribers and are ultimately responsible for Subscriber obligations under the appropriate Subscriber Agreement. Web Hosts have an obligation to provide the applicable Subscriber Agreements to their clients to inform them of their obligations.

1.1.2.1.5 VeriSign Gateway Services

Netscape and Microsoft Certificate server software permits organizations to have their own certification authorities. These organizations normally establish their CAs within a private hierarchy, and they cannot interoperate with other domains without an interoperation or root distribution arrangement. Gateway services, however, allow these CAs to enter into the VTN, and thus permit their users to interoperate with VTN Relying Parties worldwide.

Gateway Customers become CAs within the VTN when a Gateway Customer enters into an appropriate agreement with VeriSign or an Affiliate, by which one of its VTN CAs issues a Gateway Certificate to the Gateway Customer. The Gateway Certificate certifies the Gateway Customer's public key. Therefore, when a Relying Party obtains a Certificate issued by a Gateway Customer, the Relying Party is able to validate a Certificate chain with the assistance of VTN PCA Certificates securely embedded in the relying party's software. Gateway services therefore make it unnecessary for a Gateway Customer to distribute a self-signed root Certificate from its CA.

Once issued a Gateway Certificate, a Gateway Customer is akin to a Processing Center. From a secure facility, it issues, manages, and revokes Certificates. Subscribers must be Affiliated Individuals with respect to the Gateway Customer. . The Gateway program currently only covers Class 1 Certificates. Therefore, the security requirements for Gateway Customers are lower than Processing Centers, which issue multiple classes of Certificates.

1.1.2.2 Value-Added Certification Services

1.1.2.2.1 Authentication Services

VeriSign and Affiliates offer organizations authentication services, as a value-added addition to their Managed PKI services. Under these services, VeriSign or the Affiliate will confirm the identity of Certificate Applicants on behalf of Customers. One such service is performing authentication functions on behalf of Managed PKI Customers on an outsourced basis. These Managed PKI Customers may wish to outsource the authentication of all or any portion of their user base of Subscribers. For example, B2B exchanges and enterprises who already know some of their users, but not others, may find it helpful to outsource the authentication of the unknown portion of their user bases. The provision of outsourced authentication services is subject to an agreement with VeriSign or the Affiliate.

To the extent VeriSign or an Affiliate conducts certain authentication activities for the Managed PKI Customer, then VeriSign or the Affiliate would be obligated to perform the obligations in this CP of the Managed PKI Customer on its behalf. Performing such obligations, however, does not relieve the Managed PKI Customer of obligations in the CP to the extent the Managed PKI Customer retains authentication responsibilities for portions of its user base or other functions, such as initiating revocation requests.

Another value-added authentication service is the VeriSign Authentication Service Bureau program. This offering enables VeriSign and Affiliates to confirm the identity of end-user Subscribers on behalf of an organization. VeriSign and Affiliates provide this service to

organizations such as the operators of a B2B or B2C extranet or marketplace entering into an appropriate agreement for these services (“ASB Customers”). Under the Authentication Service Bureau program, VeriSign and Affiliates offer Class 2 individual Certificates (“Class 2 Individual ASB Certificates”) and Class 3 organizational Certificates used by authorized representatives of organizations interacting with the ASB Customer (“Class 3 Organizational ASB Certificates”). Because VeriSign or the Affiliate provides the authentication services as an outsourcing provider, the ASB Customer saves itself from the expense and work of implementing the policy, technology, and staffing required to confirm the identity of unknown Certificate Applicants.

Like Managed PKI, Authentication Service Bureau is an outsourcing service. ASB Customers enter into an agreement with VeriSign or an Affiliate to become a CA. This CA issues co-branded Certificates indicating that the ASB Customer is the CA. The ASB Customer, however, outsources most CA functions, both front-end and back-end, to VeriSign or the Affiliate. The one CA function that the ASB Customer retains is the obligation to initiate revocation of Certificates issued by the ASB Customer’s CA in accordance with CP § 4.4.1.1, although VeriSign or the Affiliate can also process revocation requests communicated directly to them. Except for the ASB Customer’s obligation to initiate revocation, VeriSign or the Affiliate performs all identity confirmation and Certificate lifecycle services on behalf of the ASB Customer. VeriSign or the Affiliate offering Authentication Service Bureau services (“ASB Provider”) acts as RA for the ASB Customer. An ASB Provider may either be a Processing Center or a Service Center.

1.1.2.2.2 VeriSign Digital Notarization Service

The “VeriSign Digital Notarization Service” is a service that provides a digitally signed assertion (“Digital Receipt”) that a particular document or set of data existed at a particular point in time. VeriSign acts as a third party providing assurances of time and the integrity of the document or other information. One important use of the VeriSign Digital Notarization Service is obtaining a Digital Receipt for a document embodying a business transaction, showing that the transactional document existed at a time certain. The VeriSign Digital Notarization Service responds to e-business requirements for trusted third parties, secure data archival, tamper-evident payment confirmation, and business process auditing. This service is offered exclusively to Managed PKI Customers and their Subscribers.

VeriSign has established a “Time-Stamping Authority” and “Time-Stamping Authority CA.” The Time-Stamping Authority CA has issued a special Class 3 organizational Certificate to the Time-Stamping Authority that enables the Time-Stamping Authority to digitally sign Digital Receipts.

When using the VeriSign Digital Notarization Service, the user’s client software submits a digitally signed hash of the document to the Time-Stamping Authority. The digital signature must be verifiable with reference to an Managed PKI Certificate during its Operational Period. Once received, the Time-Stamping Authority verifies the digital signature and ensures that the Managed PKI Customer has a valid account. If so, the Time-Stamping Authority creates an electronic time-stamp of the submitted data by consulting a secure source of time information. The Time-Stamping Authority then combines the time-stamp with a hash of the document to

form a data object that the Time-Stamping Authority digitally signs, thereby creating a Digital Receipt. Digital Receipts are stored by VeriSign for an application-specific period of time together with information about the document supplied by the user, and are made accessible to the appropriate parties at a later date for dispute resolution and auditing purposes, if needed. A document need not be revealed to VeriSign in order to be digitally notarized; only the hash is submitted to the VeriSign Digital Notarization service.

The Time-Stamping Authority obtains its time information from a VeriSign time server synchronized via Global Positioning Service to the Coordinated Universal Time. While the precision of the VeriSign time server is accurate within one second, due to the nature of Internet traffic, the time shown on a Digital Receipt may be 30 seconds greater or less than the actual Coordinated Universal Time.

1.1.2.2.3 NetSureSM Protection Plan

The NetSure Protection Plan is an extended warranty program that applies within VeriSign's Subdomain of the VTN and the Subdomains of participating Affiliates. Where it applies, the NetSure Protection Plan provides Subscribers receiving Retail Certificates, Class 2 Individual ASB Certificates, and Class 3 Organizational ASB Certificates with protection against accidental occurrences such as theft, corruption, loss, or unintentional disclosure of the Subscriber's private key (corresponding to the public key in the Certificate), as well as impersonation and certain loss of use of the Subscriber's Certificate. The NetSure Protection Plan also provides protection to Relying Parties when they rely on Certificates covered by the NetSure Protection Plan. NetSure is a program provided by VeriSign and backed by insurance obtained from commercial carriers. For general information concerning the NetSure Protection Plan, and a discussion of which Certificates are covered by it, see <http://www.verisign.com/netsure>.

The protections of the NetSure Protection Plan are also offered, for a fee, to Managed PKI Customers of VeriSign. They can obtain protections under the NetSure Protection Plan subject to the terms of an appropriate agreement for this service. This service not only extends the protections of the NetSure Protection Plan to the Subscribers whose Certificate Applications are approved by the Managed PKI Customer, it also extends these protections to the Managed PKI Customer itself. For example, if the Managed PKI Customer approves a Certificate Application of an employee of the Managed PKI Customer, who uses the Certificate for the business purposes of the Managed PKI Customer, and if the Subscriber's actions cause a loss, the real party bearing the loss may be the Managed PKI Customer in its role as the Subscriber's employer. If covered by the NetSure Protection Plan, the Managed PKI Customer may submit a claim for the loss sustained because of the Subscriber's actions.

1.1.2.3 Special Certificate Types

1.1.2.3.1 Wireless Certificate Services

VeriSign offers Class 3 Organizational Retail Certificates for wireless applications. VeriSign WAP server Certificates enable secure connections between servers and wireless devices such as digital cellular phones and other mobile client devices. "WAP" (Wireless Application Protocol) enables authentication and encryption between wireless Web servers and mobile devices through

“WTLS” (Wireless Transport Layer Security). WTLS is a close relative of SSL, the primary protocol used to secure the wired World Wide Web.

WTLS Certificates are used to authenticate a WTLS server to a WTLS client and to provide a basis for establishing a key to encrypt a client-server session. WTLS Certificates are like SSL server Certificates, except that the WTLS Certificates are not in the X.509 format. Rather, WTLS Certificates are smaller and simpler than X.509 Certificates to facilitate their processing in resource-constrained handsets.

1.1.2.3.2 VeriSign Managed PKI Key Management Service

Key Management Service is an optional software system installed on an enterprise premises forming part of the VeriSign Managed PKI product family. Key Management Service operates in conjunction with a VeriSign Managed PKI Service. This combination allows an enterprise manager to control the backup and recovery of user private keys and digital certificates.¹

Private keys are stored on the enterprise’s premises in encrypted form. Each Subscriber’s private key is individually encrypted with its own triple-DES symmetric key generated. A Key Escrow Record (KER) is generated, then the triple-DES key is combined with a random session key mask also generated in hardware and destroyed. Only the resulting masked session key (MSK) is securely sent and stored at VeriSign. The KER (containing the end user’s private key) and the random session key mask are stored in the Key Manager database on the enterprise premises.

Recovery of a private key and digital certificate requires the Managed PKI administrator to securely log on to the Managed PKI Control Center, select the appropriate key pair to recover and click a “recover” hyperlink. Only after an approved administrator clicks the “recover” link is the MSK for that key pair returned from the Managed PKI database operated out of VeriSign’s secure data center. The Key Manager combines the MSK with the random session key mask and regenerates the triple-DES key which was used to originally encrypt the private key, allowing recovery of the end user’s private key. As a final step, an encrypted PKCS#12 file is returned to the administrator and ultimately distributed to the end user.

An enterprise using KMS shall, at a minimum:

- Notify the subscribers that their private keys are escrowed
- Protect subscribers’ escrowed keys from unauthorized disclosure,
- Protect all information, including the administrator’s own key(s) that could be used to recover subscribers’ escrowed keys.
- Release subscribers’ escrowed keys only for properly authenticated and authorized requests for recovery.
- Revoke the Subscriber’s Key pair prior to recovering the encryption key.

¹ VeriSign may, in limited circumstances, host KMS on behalf of an enterprise customer. In such a scenario KMS will operate as described in section 1.1.2.3.2 except that the portion normally hosted by the enterprise will be hosted in a secure VeriSign facility. The only person authorized to recover escrowed encryption keys on behalf of the enterprise is the enterprise Administrator(s). The Key Manager database shall be located in a separate physical location from the database storing the MSK. VeriSign’s access to the Key Manager database shall be restricted to Trusted Persons only, using dual username and password access control.

- Not be required to communicate any information concerning a key recovery to the subscriber except when the subscriber him/herself has requested recovery.
- Not disclose or allow to be disclosed escrowed keys or escrowed key-related information to any third party unless required by the law, government rule, or regulation; by the enterprise's organization policy; or by order of a court of competent jurisdiction.

1.1.2.3.3 VeriSign Roaming Service

The "VeriSign Roaming Service," offered to Managed PKI Customers, enables a Subscriber to digitally sign critical transactions, such as stock trades, and obtain access to confidential information, without being bound to a single client terminal on which his or her private key resides. Roaming is becoming common in many workplace environments and increasingly prevalent in consumer environments, such as public kiosks. Developed by VeriSign's research team in consultation with RSA Laboratories, VeriSign's roaming technology permits Subscribers using the service ("Roaming Subscribers") to download their private keys and conduct private key operations on different client terminals. The Managed PKI Customer need not distribute and support smart cards or other hardware tokens.

The Roaming Subscriber can use his or her private key from any client terminal. The VeriSign Roaming Service encrypts Roaming Subscribers' private keys with symmetric keys that are split and stored on one server or two servers in two physical locations to protect against attacks on a single credential server. The private key itself is stored in encrypted form on the Enterprise Roaming Server. The Roaming Subscriber authenticates himself or herself to the server(s) using a password, and assuming the password is successfully provided, the encrypted private key and the components of the symmetric key needed to decrypt the Subscriber's private key are downloaded to the client terminal. At the client terminal, the symmetric key is reconstituted, the Subscriber's private key is decrypted, and the private key is then available for use during a single session. Following the session, the private key on the client terminal is deleted such that it is unrecoverable.

1.2 Identification

VeriSign, acting as a policy-defining authority, has assigned the Certificate policy within this CP for each Class of Certificate an object identifier value extension and set forth in this section. The object identifier values used for the three Classes of end-user Subscriber Certificates are:

- The Class 1 Certificate Policy: VeriSign/pki/policies/vtn-cp/class1 (2.16.840.1.113733.1.7.23.1).
- The Class 2 Certificate Policy: VeriSign/pki/policies/vtn-cp/class2 (2.16.840.1.113733.1.7.23.2).
- The Class 3 Certificate Policy: VeriSign/pki/policies/vtn-cp/class3 (2.16.840.1.113733.1.7.23.3).

These object identifiers for end-user Subscriber Certificates correspond to the appropriate Class.

1.3 Community and Applicability

The community governed by this CP is the VeriSign Trust Network. The VTN is a PKI that accommodates a worldwide, large, public, and widely distributed community of wired and

wireless users with diverse needs for communications and information security. The VTN is the public domain governed by this CP, and the CP is the document that governs the VTN.

1.3.1 Certification Authorities

The term Certification Authority is an umbrella term that refers to all entities issuing Certificates within the VTN. The CA term encompasses a subcategory of issuers called Primary Certification Authorities. PCAs act as roots of three domains, one for each class of Certificate. Each PCA is a VeriSign entity. Subordinate to the PCAs are Certification Authorities that issue Certificates to end-user Subscribers or other CAs. CAs also fall into five categories: (1) Processing Centers, (2) Client Service Centers, (3) Managed PKI Customers, (4) Gateway Customers, and (5) ASB Customers.

Processing Centers in the Consumer and Web Site lines of business are CAs that perform both RA front-end functions and back-end functions, unless front-end functions are delegated to an RA. Processing Centers in the Enterprise line of business are outsource providers performing CA functions for Managed PKI Customers. RA front-end functions include establishing enrollment procedures, confirming identity, approving or denying Certificate Applications, initiating revocations, and approving or denying requests to renew Certificates. Back-end functions include issuing, managing, revoking, and renewing Certificates from a secure facility protecting CA private keys. VeriSign is a Processing Center that hosts all VTN PCAs and certain CAs in its secure CA facility. Affiliates may also establish a Processing Center with approval by VeriSign.

Client Service Centers, by contrast, are Affiliates acting as CAs that do not have their own Processing Centers. They perform RA front-end functions but outsource to a Processing Center, either VeriSign or a Processing Center Affiliate, their back-end functions. Managed PKI Customers, like Service Centers, become CAs within the VTN. Like Client Service Centers, Managed PKI Customers outsource back-end functions to a Processing Center, while retaining RA functions for themselves. Gateway Customers use Netscape or Microsoft Certificate server software to issue Class 1 Certificates. Gateway Customers perform both front-end and back-end functions. Finally, ASB Customers contract with VeriSign or an Affiliate to become a CA, which issues Certificates naming the ASB Customer as the CA. ASB Customers, however, outsource to VeriSign or an Affiliate ASB Provider all front-end and back-end functions, except for the obligation to initiate revocation of Certificates issued by the ASB Customer's CA in accordance with CP § 4.4.1.1.

One VTN CA technically outside the three hierarchies under each of the PCAs is the RSA Secure Server Certification Authority, which VeriSign acquired from RSA Security Inc. The RSA Secure Server CA does not have a superior CA, such as a root or a PCA. Rather, the RSA Secure Server CA acts as its own root and has issued itself a self-signed root Certificate. It also issues Certificates to end-user Subscribers. Thus, the RSA Secure Server Hierarchy consists only of the RSA Secure Server CA. The RSA Secure Server CA issues Secure Server IDs, which are deemed to be Class 3 Organizational Certificates.

Although the RSA Secure Server CA is not certified under the Class 3 PCA, the Certificates it issues are functionally equivalent to Certificates issued by a Class 3 CA. The RSA Secure

Server CA employs lifecycle practices that are substantially similar with those of other Class 3 CAs within the VTN. Thus, VeriSign has approved and designated the RSA Secure Server Certification Authority as a Class 3 CA within the VTN. The Certificates it issues, Secure Server IDs, are considered to provide assurances of trustworthiness comparable to other Class 3 organizational Certificates.

1.3.2 Registration Authorities

RAs assist a CA by performing front-end functions of confirming identity, approving or denying Certificate Applications, requesting revocation of Certificates, and approving or denying renewal requests. VTN RAs fall into five categories: (1) Server Service Centers, (2) Managed PKI, (3) Managed PKI Lite Customers, (4) Managed PKI for SSL Customers, (5) Managed PKI for SSL Premium Edition Customers, and (6) ASB Providers. Other types of RAs are permitted with VeriSign's advance written consent and if these RAs meet the obligations placed on Managed PKI Customers, subject to any modifications necessary to account for any differences between Managed PKI technology and the technology used by these RAs and the terms of an appropriate agreement.

Server Service Centers are Service Centers that approve Certificate Applications for server Certificates (Secure Server IDs and Global Server IDs). They act as an RA assisting a VeriSign CA to issue these Certificates. These VeriSign CAs include the RSA Secure Server CA, which issues Secure Server IDs, and the VeriSign Class 3 Universal Strong Encryption CA, which issues Global Server IDs. Managed PKI Lite Customers become RAs assisting a VeriSign or Affiliate CA to issue client Certificates to end-user Subscribers. Similarly, Managed PKI for SSL Customers and Managed PKI for SSL Premium Edition Customers become RAs using Managed PKI that assist the RSA Secure Server CA, the VeriSign Class 3 Universal Strong Encryption CA, or similar VeriSign CA to issue Secure Server IDs or Global Server IDs. ASB Providers (VeriSign or an Affiliate) offer Authentication Service Bureau services to ASB Customers. ASB Providers perform both RA front-end functions and back-end functions for ASB Customer CAs.

1.3.3 End Entities

Class 1 and 2 Certificates are client Certificates issued only to individual end-user Subscribers. Class 3 Certificates may be issued to individuals, and other types of Class 3 Certificates may be issued to organizations. Class 1-2 Certificates and Class 3 individual Certificates may either be Retail Certificates or Managed PKI Certificates. In addition, Class 2 Individual ASB Certificates are offered through the Authentication Service Bureau. Retail Certificates may be issued to the public generally. Except under the Two-Tier Authentication Service described in CP § 1.1.2.1.1, individuals obtaining Managed PKI Certificates must be affiliated with the Managed PKI Customer that approved their Certificate Applications or their designee as an "Affiliated Individual." Affiliated Individuals are natural persons that are related to a Managed PKI Customer or Managed PKI Lite Customer entity (i) as an officer, director, employee, partner, contractor, intern, or other person within the entity, (ii) as a member of a VeriSign registered community of interest, or (iii) as a person maintaining a relationship with the entity where the entity has business or other records providing appropriate assurances of the identity of such person (*e.g.*, a customer).

Managed PKI Customers obtaining services under the Two-Tier Authentication Service delegate RA functions to another organization with which it has a relationship. Individuals obtaining Managed PKI Certificates must be affiliated with the organization that has been delegated these RA functions as an Affiliated Individual.

Class 3 Administrator Certificates are special-purpose and limited-use Certificates that the authorized administrator of VeriSign, an Managed PKI Customer, or Affiliate uses exclusively to perform Administrator functions. Administrators who use these Certificates are Trusted Persons who perform Certificate management functions on behalf of Processing Centers, Service Centers, or Managed PKI Customers.

In addition to client Certificates issued to individuals, Class 3 Certificates also include Certificates issued to organizational end-user Subscribers. Class 3 Organizational ASB Certificates are issued to an organization, whose private key is controlled by an authorized representative of the organization. Authentication procedures confirm that the representative has the authority to act on behalf of the organization. Aside from Class 3 Organizational ASB Certificates, organizational Class 3 Certificates are issued to devices, including:

- Web servers (Secure Server IDs and Global Server IDs),
- ,
- OFX servers, and
- Devices digitally signing code and other content.

This list of Subscribers of Class 3 organizational Certificates is not exhaustive.

Secure Server IDs and Global Server IDs may either be Retail Certificates or Managed PKI Certificates. Retail Secure Server IDs and Global Server IDs will be issued directly to an organization by VeriSign after VeriSign or an Affiliate approves the Subscriber's Certificate Application. Secure Server IDs and Global Server IDs that are Managed PKI Certificates will be issued by VeriSign following the approval of the Certificate Application by a Managed PKI for SSL Customer or Managed PKI for SSL Premium Edition Customer.

CAs are themselves, as a technical matter, Subscribers of Certificates, either as a PCA issuing a self-signed Certificate to itself, or as a CA issued a Certificate by a superior CA. References to "Subscribers" in this CP, however, apply only to end-user Subscribers.

1.3.4 Applicability

This CP applies to all VTN Participants, including VeriSign, Affiliates, Customers, Universal Service Centers, Resellers, Subscribers, and Relying Parties. This CP sets forth policies governing the use of Certificates in each of Classes 1-3. Each Class of Certificate is generally appropriate for use with the applications set forth in CP § 1.3.4.1. Nonetheless, by contract or within specific environments (such as an intra-company environment), VTN Participants are permitted to use Certificates for higher security applications than the ones described in CP §§ 1.1.1, 1.3.4.1. Any such usage, however, shall be limited to such entities and subject to CP §§ 2.2.1.2, 2.2.2, and these entities shall be solely responsible for any harm or liability caused by such usage.

1.3.4.1 Suitable Applications

The subsections within this section list suitable applications for VTN Certificates by Class. This listing, however, is not intended to be exhaustive.

Individual Certificates and some organizational Certificates permit Relying Parties to verify digital signatures. VTN Participants acknowledge and agree, to the extent permitted by applicable law, that where a transaction is required to be in writing, a message or other record bearing a digital signature verifiable with reference to a VTN Certificate is valid, effective, and enforceable to an extent no less than had the same message or record been written and signed on paper. Subject to applicable law, a digital signature or transaction entered into with reference to a VTN Certificate shall be effective regardless of the geographic location where the VTN Certificate is issued or the digital signature created or used, and regardless of the geographic location of the place of business of the CA or Subscriber.

VeriSign periodically rekeys Intermediate CAs. Third party applications or platforms that have an Intermediate CA embedded as a root certificate may not operate as designed after the Intermediate CA has been rekeyed. VeriSign therefore does not warrant the use of Intermediate CAs as root certificates and recommends that Intermediate CAs not be embedded into applications and/or platforms as root certificates. VeriSign recommends the use of PCA Roots as root certificates.

1.3.4.1.1 Class 1 Certificates

Class 1 Certificates are suitable for modestly enhancing the security of e-mail through the use of digital signatures and confidentiality encryption where the e-mail requires a low level of assurances compared to Class 2 and 3. They do not provide an assurance of identity of the Subscriber, though. Therefore, a digital signature made with a private key corresponding to the public key in a Class 1 Certificate using the S/MIME protocol cannot be used for authentication purposes or to support Non-repudiation. Rather, the digital signature function is appropriate as a means of ensuring, when e-mail correspondents are having a series of ongoing communications, that the communications are continuing to originate from the same person and that they have not been modified without detection since they were digitally signed. The digital signature also provides modest assurances that the e-mail originated from a sender with a certain e-mail address. The Certificate, however, provides no proof of who that sender using that e-mail address actually is. The encryption application enables a Relying Party to use the Subscriber's Certificate to encrypt messages to the Subscriber, although the sending Relying Party cannot be sure that the recipient is in fact the person named in the Certificate.

Class 1 Certificates can also be used for client authentication during online sessions. The web site or other device can use the Certificate to ensure, over a series of sessions, that the sessions are being initiated by the same Subscriber having a certain e-mail address. Again, however, the Certificate provides no proof of who that Subscriber actually is.

1.3.4.1.2 Class 2 Certificates

Class 2 Certificates are suitable for securing some inter- and intra-organizational, commercial, and personal e-mail requiring a medium level of assurances, in relation to Class 1 and 3. The use of digital signatures with the S/MIME protocol permits the authentication of the identity of e-mail correspondents, message integrity, and support for Non-repudiation. In addition, S/MIME permits Class 2 Certificates to be used for the exchange and/or encryption of session keys to encrypt e-mails. Class 2 Certificates are also appropriate for client authentication, where the web site or other device requires a medium-assurance proof of identity in comparison with Class 1 and 3. Client authentication may, for example, provide access control to protected databases or web sites.

1.3.4.1.3 Class 3 Certificates

Class 3 Individual Certificates

Class 3 Certificates are suitable for securing most inter- and intra-organizational, commercial, and personal e-mail requiring a high level of security in comparison with Class 1 and 2. The use of digital signatures with the S/MIME protocol permits the authentication of the identity of e-mail correspondents, message integrity, and support for Non-repudiation. In addition, S/MIME permits Class 3 Certificates to be used for the exchange and/or encryption of session keys to encrypt e-mails. Class 3 Certificates are also appropriate for client authentication, for example for access control, where the web site or other device requires high-assurance proof of identity in comparison with Class 1 and 2.

VeriSign issues special Class 3 client Certificates to Administrators (“Administrator Certificates”) who approve Certificate Applications on behalf of Processing Centers, Service Centers, and Managed PKI Customers. Administrator Certificates are used for Administrator functions. That is, Administrators may use Administrator Certificates for performing functions such as approving or denying Certificate Applications, initiating revocation requests, and approving or denying renewals of the Certificates of end-user Subscriber Certificates or the Certificates of other Administrators.

Class 3 Organizational Certificates

Table 3 summarizes the most common kinds of Class 3 organizational Certificates offered within the VTN, each of which is described below. Note that this table is not an exhaustive list of Class 3 organizational Certificates.

<i>Types of Class 3 Organizational Certificates</i>	<i>Functions</i>	<i>Applicable Security Protocols and Technology</i>
Secure Server IDs	Server authentication, confidentiality encryption, and, when communicating with other servers, client authentication	SSL
Global Server IDs	Server authentication, confidentiality encryption, and, when communicating with other	SSL and Server Gated Cryptography

<i>Types of Class 3 Organizational Certificates</i>	<i>Functions</i>	<i>Applicable Security Protocols and Technology</i>
	servers, client authentication	
OFX Certificates	Server authentication and confidentiality encryption	SSL and Open Financial Exchange standard
Certificates for code and other content signing	Authentication and integrity	Various technologies
Class 3 Organizational ASB Certificate	Digital signatures, message integrity, confidentiality encryption, client authentication	Authentication Service Bureau technology

Table 3 – Types of Organizational Class 3 Certificates

A Secure Server ID permits web browsers to authenticate the identity of the Subscriber’s web server and to create an encrypted channel between the browser and the Subscriber’s server using the SSL protocol. Global Server IDs are a special kind of server Certificate which, in addition to performing the foregoing functions, assist the web server in establishing strong cryptographic protection for their SSL sessions with the server. Global Server IDs may even make strong cryptographic protection possible for so-called “export grade” browsers that, absent a Global Server ID, are limited to using 40-bit encryption.

An additional type of Class 3 organizational Certificate is the Open Financial Exchange (“OFX”) Certificate. OFX is a standard for the exchange of electronic financial data among financial institutions, businesses, and consumers over the Internet. OFX facilitates consumer and small business banking, bill presentment and payment, and the investing of stocks, bonds, and mutual funds.

Businesses using OFX set up a server to communicate with customers. An OFX Certificate permits the creation of SSL connections between the server and the client. As with Secure Server IDs and Global Server IDs, OFX Certificates’ use of SSL authenticates the server to the client, provides message integrity, and encrypts communications between the server and the client.

The VTN offers Class 3 code or other content signing Certificates intended for organizations to digitally sign code or other content. The purpose of these certificates is to authenticate the source of the code or content and to provide assurances of integrity of this content. That is, these Certificates provide assurances that the code or content came from the appropriate developer or source purporting to provide it, and that the code content was not tampered with, for example to introduce malicious code into it. Any CA issuing such certificates, however, does not endorse the use of any code or content of the Subscribers of these Certificates. Any such CA would not be involved with the functionality of the code or content signed, the products or services offered, or the customer support functions of these Subscribers.

Finally, Class 3 Organizational ASB Certificates permit an authorized representative of an organization to act on behalf of the organization. They are suitable for inter- and intra-organizational and commercial e-mail using digital signatures and confidentiality encryption, as

well as client authentication, in which the sender or user is considered to be an organization rather than an individual, and where a high level of security is required in comparison with Class 1 and 2.

1.3.4.2 Restricted Applications

In general, VTN Certificates are general-purpose Certificates. VTN Certificates may be used globally and to interoperate with diverse Relying Parties worldwide. Usage of VTN Certificates is not generally restricted to a specific business environment, such as a pilot, financial services system, vertical market environment, or virtual marketplace. Nonetheless, such use is permitted and Customers using Certificates within their own environment may place further restrictions on Certificate use within these environments. VeriSign and other VTN Participants, however, are not responsible for monitoring or enforcing any such restrictions in these environments.

Nonetheless, certain VTN Certificates are limited in function. For example, CA Certificates may not be used for any functions except CA functions. Moreover, client Certificates are intended for client applications and shall not be used as server or organizational Certificates. In addition, Class 3 organizational Certificates issued to devices are limited in function to web servers and to secure SSL/TLS sessions (in the case of Secure Server IDs and Global Server IDs), OFX (in the case of OFX Certificates), and object signing (in the case of object signing Certificates). Further, Administrator Certificates shall only be used to perform Administrator functions.

Also, with respect to X.509 Version 3 VTN Certificates, the key usage extension is intended to limit the technical purposes for which a private key corresponding to the public key in a Certificate may be used within the VTN. *See* CP § 6.1.9. In addition, end-user Subscriber Certificates shall not be used as CA Certificates. This restriction is confirmed by the absence of a Basic Constraints extension. *See* CP § 7.1.2.4. The effectiveness of extension-based limitations, however, is subject to the operation of software manufactured or controlled by entities other than VeriSign.

More generally, Certificates shall be used only to the extent use is consistent with applicable law, and in particular shall be used only to the extent permitted by applicable export or import laws.

1.3.4.3 Prohibited Applications

VTN Certificates are not designed, intended, or authorized for use or resale as control equipment in hazardous circumstances or for uses requiring fail-safe performance such as the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control systems, or weapons control systems, where failure could lead directly to death, personal injury, or severe environmental damage. Also, subject to CP § 1.3.4, Class 1 Certificates shall not be used as proof of identity or as support of nonrepudiation of identity or authority.

1.4 Contact Details

1.4.1 Specification Administration Organization

The organization administering this CP is the VTN Policy Management Authority. The address for the PMA is:

VeriSign Trust Network Policy Management Authority
c/o VeriSign, Inc.
487 E. Middlefield Road
Mountain View, CA 94043 USA
+1 (650) 961-7500 (voice)
+1 (650) 426-7300 (fax)
practices@verisign.com

1.4.2 Contact Person

Address inquiries about the CP to cp@verisign.com or to the following address:

VeriSign, Inc.
487 E. Middlefield Road
Mountain View, CA 94043 USA
Attn: Practices and External Affairs – CP
+1 (650) 961-7500 (voice)
+1 (650) 426-7300 (fax)
practices@verisign.com

1.4.3 Person Determining CPS Suitability for the Policy

The persons determining whether the CPS of an Affiliate is suitable for this CP are the members of the PMA. *See* CP § 1.4.2.

2. General Provisions

2.1 Obligations (Class 1-3)

2.1.1 CA Obligations

CAs shall perform the specific obligations appearing throughout this CP. The provisions of the CP specify obligations of each category of CAs: Processing Centers, Client Service Centers, Managed PKI Customers, Gateway Customers, and ASB Customers.

In addition, VeriSign and Affiliates shall use commercially reasonable efforts to ensure that Subscriber Agreements and Relying Party Agreements bind Subscribers and Relying Parties within their respective Subdomains. Examples of such efforts include, but are not limited to, requiring assent to a Subscriber Agreement as a condition of enrollment or requiring assent to a Relying Party Agreement as a condition of receiving Certificate status information. The Subscriber Agreements and Relying Party Agreements of VeriSign and Affiliates shall meet the

requirements of the Affiliate Practices Legal Requirements Guidebook. Similarly, Universal Service Centers and Resellers (where required by contract) shall use Subscriber Agreements and Relying Party Agreements in accordance with the requirements imposed by VeriSign or the applicable Affiliate. The Subscriber Agreements and Relying Party Agreements used by VeriSign, Affiliates, Universal Service Centers, and Resellers shall include the provisions required by CP §§ 2.2-2.4.

Managed PKI Customers and Gateway Customers are permitted to use Subscriber Agreements specific to them, although not required to do so. Managed PKI Customers and Gateway Customers using Subscriber Agreements shall include the provisions required by CP §§ 2.2-2.4. If a Managed PKI Customer, Gateway Customer, or Reseller does not use its own Subscriber Agreement, the Subscriber Agreement of VeriSign or the applicable Affiliate shall apply. If a Reseller has no Relying Party Agreement, the Relying Party Agreement of VeriSign or the applicable Affiliate shall apply.

2.1.2 RA Obligations

RAs assist a Processing Center or Service Center CA by performing validation functions, approving or rejecting Certificate Applications, requesting revocation of Certificates, and approving renewal requests. The provisions of the CP specify obligations of each category of RAs: Server Service Centers, Managed PKI Lite Customers, Managed PKI for SSL Customers, Managed PKI for SSL Premium Edition Customers, and ASB Providers.

Also, Server Service Centers and ASB Providers shall ensure that Subscriber Agreements and Relying Party Agreements bind Subscribers and Relying Parties within their respective Subdomains in accordance with CP § 2.1.1. This requirement does not apply to other RAs.

2.1.3 Subscriber Obligations

Certificate Applicants shall provide complete and accurate information on their Certificate Applications and shall manifest assent to the applicable Subscriber Agreement as a condition of obtaining a Certificate.

Subscribers shall perform Subscriber functions in accordance with the specific obligations appearing throughout this CP. Subscribers shall use their Certificates in accordance with CP § 1.3.4. Subscribers shall protect their private keys in accordance with CP §§ 6.1-6.2, 6.4. If a Subscriber discovers or has reason to believe there has been a Compromise of the Subscriber's Private Key or the activation data protecting such Private Key, or the information within the Certificate is incorrect or has changed, the Subscriber shall promptly:

- Notify the entity that approved the Subscriber's Certificate Application, either a CA or an RA, in accordance with CP § 4.4.1.1 and request revocation of the Certificate in accordance with CP §§ 3.4, 4.4.3.1, and
- Notify any person that may reasonably be expected by the Subscriber to rely on or to provide services in support of the Subscriber's Certificate or a digital signature verifiable with reference to the Subscriber's Certificate.

Subscribers shall cease use of their private keys at the end of their key usage periods under CP § 6.3.2.

Subscribers shall not monitor, interfere with, or reverse engineer the technical implementation of the VTN, except upon prior written approval from VeriSign, and shall not otherwise intentionally compromise the security of the VTN.

2.1.4 Relying Party Obligations

Before any act of reliance, Relying Parties shall independently assess the appropriateness of the use of a Certificate for any given purpose and determine that the Certificate will, in fact, be used for an appropriate purpose. VeriSign, CAs, and RAs are not responsible for assessing the appropriateness of the use of a Certificate. More specifically, Relying Parties shall not use Certificates beyond the limitations in CP § 1.3.4.2 and for purposes prohibited in CP § 1.3.4.3.

Assuming that the use of the Certificate is appropriate, Relying Parties shall utilize the appropriate software and/or hardware to perform digital signature verification or other cryptographic operations they wish to perform, as a condition of relying on Certificates in connection with each such operation. Such operations include identifying a Certificate Chain and verifying the digital signatures on all Certificates in the Certificate Chain. Relying Parties shall not rely on a Certificate unless these verification procedures are successful.

Relying Parties shall also check the status of a Certificate on which they wish to rely, as well as all the Certificates in its Certificate Chain in accordance with CP §§ 4.4.10, 4.4.12. If any of the Certificates in the Certificate Chain have been revoked, the Relying Party shall not rely on the end-user Subscriber Certificate or other revoked Certificate in the Certificate Chain.

Finally, Relying Parties must assent to the terms of a Subscriber Agreement or Relying Party Agreement as a condition of using or otherwise relying on Certificates. Relying Parties that are also Subscribers agree to be bound by Relying Party terms, disclaimers of warranty, and limitations of liability when they agree to a Subscriber Agreement.

If all of the checks described above are successful, the Relying Party shall be entitled to rely on the Certificate, provided that reliance upon the Certificate is reasonable under the circumstances. If the circumstances indicate a need for additional assurances, the Relying Party must obtain such assurances for such reliance to be deemed reasonable.

Relying Parties shall not monitor, interfere with, or reverse engineer the technical implementation of the VTN, except upon prior written approval from VeriSign, and shall not otherwise intentionally compromise the security of the VTN.

2.1.5 Repository Obligations

In the VTN, there is no separate entity providing repository services. Rather, VeriSign and Affiliates are responsible for repository functions as follows: Processing Centers have a repository for their own CAs, and the CAs of their Managed PKI Customers, Gateway Customers, and ASB Customers. Service Centers have a repository for their own CAs, and the CAs of their Managed PKI Customers, Gateway Customers, and ASB Customers, but as part of

their contract with a Processing Center, the Processing Center hosts that repository on behalf of the Service Center.

Gateway Customers and Processing Centers issuing Certificates to end-user Subscribers shall publish Certificates they issue in the repository set forth in Table 4 in accordance with CP § 2.6.

<i>CA</i>	<i>Entity Issuing the Certificate on Behalf of the CA</i>	<i>Applicable Repository</i>
Processing Center	The Processing Center	The Processing Center's own repository
Client Service Center	Processing Center	The Service Center's repository accessible from its web site hosted by the Processing Center
Managed PKI Customer or ASB Customer of a Processing Center	Processing Center	The Processing Center's repository
Managed PKI Customer or ASB Customer of a Service Center	Processing Center	The Service Center's repository accessible from its web site hosted by the Processing Center
Gateway Customer of a Processing Center	The Gateway Customer	The Processing Center's repository
Gateway Customer of a Service Center	The Gateway Customer	The Service Center's repository accessible from its web site hosted by the Service Center's Processing Center

Table 4 – Applicable Repositories by Type of CA

Upon revocation of an end-user Subscriber's Certificate, the Processing Center or Gateway Customer that issued the Certificate shall publish notice of such revocation in the repository required by Table 4. In addition, Processing Centers shall issue CRLs and provide Online Certificate Status Protocol ("OCSP") services (to the extent they offer OCSP services) for their own CAs and the CAs of Service Centers, Managed PKI Customers, Gateway Customers, and ASB Customers within their Subdomains, pursuant to CP §§ 4.4.9, 4.4.11.

2.2 Liability (Class 1-3)

2.2.1 Certification Authority Liability

The warranties, disclaimers of warranty, and limitations of liability among VeriSign, Affiliates, Universal Service Centers, Resellers, and their respective Customers are set forth and governed by the agreements among them. This CP § 2.2.1 relates only to the warranties that certain CAs (Processing Centers, Client Service Centers, Managed PKI Customers, Gateway Customers) must make to end-user Subscribers receiving Certificates from them and to Relying Parties, the

disclaimers of warranties they shall make to such Subscribers and Relying Parties, and the limitations of liability they shall place on such Subscribers and Relying Parties. Since ASB Customers outsource all front-end and back-end functions to the ASB Provider, the warranty requirements of this section do not apply to ASB Customers.

VeriSign, Affiliates, Universal Service Centers, and (where required) Resellers shall use Subscriber Agreements and Relying Party Agreements in accordance with CP § 2.1.1. Managed PKI Customers and Gateway Customers have the option of using a Subscriber Agreement. These Subscriber Agreements and Relying Party Agreements shall meet the requirements of the Affiliate Practices Legal Requirements Guidebook (in the case of VeriSign and Affiliates) and the requirements imposed by VeriSign or the Affiliate (in the case of Universal Service Centers and Resellers). Requirements that Subscriber Agreements contain warranties, disclaimers, and limitations of liability below apply to VeriSign, Affiliates, Universal Service Centers, and those Managed PKI Customers, Gateway Customers, and Resellers that use Subscriber Agreements. Requirements concerning warranties, disclaimers, and limitations in Relying Party Agreements shall apply to VeriSign, Affiliates, Universal Service Centers, and those Resellers that use Relying Party Agreements. Note that terms applicable to Relying Parties shall also be included in Subscriber Agreements, in addition to Relying Party Agreements, because Subscribers often act as Relying Parties as well.

2.2.1.1 Certification Authority Warranties to Subscribers and Relying Parties

Subscriber Agreements shall include a warranty to Subscribers that:

- There are no material misrepresentations of fact in the Certificate known to or originating from the entities approving the Certificate Application or issuing the Certificate,
- There are no errors in the information in the Certificate that were introduced by the entities approving the Certificate Application or issuing the Certificate as a result of a failure to exercise reasonable care in managing the Certificate Application or creating the Certificate,
- Their Certificates meet all material requirements of the applicable CPS, and
- Revocation services and use of a repository conform to the applicable CPS in all material aspects.

Relying Party Agreements shall contain a warranty to Relying Parties who reasonably rely on a Certificate that:

- All information in or incorporated by reference in such Certificate, except Nonverified Subscriber Information, is accurate,
- In the case of Certificates appearing in a repository, that the Certificate has been issued to the individual or organization named in the Certificate as the Subscriber, and that the Subscriber has accepted the Certificate in accordance with CP § 4.3, and
- The entities approving the Certificate Application and issuing the Certificate have substantially complied with the applicable CPS when issuing the Certificate.

In addition to these warranties, VeriSign's NetSure Protection Plan provides warranties to Subscribers who have obtained Certificates subject to the NetSure Protection Plan within VeriSign's Subdomain or the Subdomains of participating Affiliates. These additional

warranties cover Subscribers' activities when they act as Relying Parties. For more information about the NetSure Protection Plan, see CP § 1.1.2.2.3.

2.2.1.2 Certification Authority Disclaimers of Warranties

To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements shall disclaim VeriSign's and the applicable Affiliate's possible warranties, including any warranty of merchantability or fitness for a particular purpose, outside the context of the NetSure Protection Plan.

2.2.1.3 Certification Authority Limitations of Liability

To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements shall limit VeriSign's and the applicable Affiliates' liability outside the context of the NetSure Protection Plan. Limitations of liability shall include an exclusion of indirect, special, incidental, and consequential damages. They shall also include the following liability caps limiting VeriSign's and the Affiliate's damages concerning a specific Certificate:

<i>Class</i>	<i>Liability Caps</i>
Class 1	One Hundred U.S. Dollars (\$ 100.00 US)
Class 2	Five Thousand U.S. Dollars (\$ 5,000.00 US)
Class 3	One Hundred Thousand U.S. Dollars (\$ 100,000.00 US)

Table 5 – Liability Caps

Note: The liability caps in Table 5 limit damages recoverable outside the context of the NetSure Protection Plan. Amounts paid under the NetSure Protection Plan are subject to their own liability caps. The liability caps under the NetSure Protection Plan for different kinds of Certificates range from \$1,000 US to \$1,000,000 US. See the NetSure Protection Plan for more detail at <http://www.verisign.com/repository/netsure/>.

2.2.1.4 Force Majeure

To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements shall include a force majeure clause protecting VeriSign and the applicable Affiliate.

2.2.2 Registration Authority Liability

The warranties, disclaimers of warranty, and limitations of liability between an RA and the CA it is assisting to issue Certificates, or the applicable Universal Service Center or Reseller, are set forth and governed by the agreements between them. VeriSign, Affiliates, and ASB Providers shall use Subscriber Agreements and Relying Party Agreements in accordance with CP §§ 2.1.1-2.1.2, which have their own warranties, disclaimers, and limitations. This CP § 2.2.2 relates only to the warranties, disclaimers of warranty, and limitations of liability that Server Service Center and ASB Provider RAs must apply to end-user Subscribers whose Certificate Applications they approve and Relying Parties relying on Certificates resulting from the Certificate Applications they approve.

Managed PKI Lite Customers, Managed PKI for SSL Customers, and Managed PKI for SSL Premium Edition Customers do not use Subscriber Agreements or Relying Party Agreements. Thus, the requirements of this section do not apply to them. Rather, the Subscriber Agreement of the Superior Entity of the Managed PKI Lite Customer, Managed PKI for SSL Customer, or Managed PKI for SSL Premium Edition Customer (*i.e.*, VeriSign or an Affiliate) shall apply.

Server Service Centers and ASB Providers, on behalf of their ASB Customer CAs, shall include within Subscriber Agreements and Relying Party Agreements the warranties, disclaimers of warranty, limitations of liability, and force majeure clauses required by CP §§ 2.2.1.1-2.2.1.4.

2.2.3 Subscriber Liability

2.2.3.1 Subscriber Warranties

Subscriber Agreements shall require Subscribers to warrant that:

- Each digital signature created using the private key corresponding to the public key listed in the Certificate is the digital signature of the Subscriber and the Certificate has been accepted and is operational (not expired or revoked) at the time the digital signature is created,
- No unauthorized person has ever had access to the Subscriber's private key,
- All representations made by the Subscriber in the Certificate Application the Subscriber submitted are true,
- All information supplied by the Subscriber and contained in the Certificate is true,
- The Certificate is being used exclusively for authorized and legal purposes, consistent with the applicable CPS, and
- The Subscriber is an end-user Subscriber and not a CA, and is not using the private key corresponding to any public key listed in the Certificate for purposes of digitally signing any Certificate (or any other format of certified public key) or CRL, as a CA or otherwise.

Where a Subscriber's Certificate Application was approved by a Managed PKI Customer using the Managed PKI Key Manager offering, however, the Subscriber warrants only that no unauthorized person has ever had access to the copy of the Subscriber's private key on the Subscriber's hardware/software platform. These Subscribers make no warranty concerning the copies of their private keys in the possession of the Managed PKI Customers using Managed PKI Key Manager.

2.2.3.2 Private Key Compromise

This CP sets forth VTN Standards for the protection of the private keys of Subscribers. *See* CP § 6.2.7.1. Subscriber Agreements shall state that Subscribers failing to meet these VTN Standards are solely responsible for any loss or damage resulting from such failure.

2.2.4 Relying Party Liability

Subscriber Agreements and Relying Party Agreements shall require Relying Parties to acknowledge that they have sufficient information to make an informed decision as to the extent to which they choose to rely on the information in a Certificate, that they are solely responsible for deciding whether or not to rely on such information, and that they shall bear the legal consequences of their failure to perform the Relying Party obligations in CP 2.1.4.

2.3 Financial Responsibility (Class 1-3)

2.3.1 Indemnification by Subscribers and Relying Parties

2.3.1.1 Indemnification by Subscribers

To the extent permitted by applicable law, Subscriber Agreements shall require Subscribers to indemnify VeriSign and any non-VeriSign CAs or RAs for:

- Falsehood or misrepresentation of fact by the Subscriber on the Subscriber's Certificate Application,
- Failure by the Subscriber to disclose a material fact on the Certificate Application, if the misrepresentation or omission was made negligently or with intent to deceive any party,
- The Subscriber's failure to protect the Subscriber's private key, to use a Trustworthy System, or to otherwise take the precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of the Subscriber's private key, or
- The Subscriber's use of a name (including without limitation within a common name, domain name, or e-mail address) that infringes upon the Intellectual Property Rights of a third party.

2.3.1.2 Indemnification by Relying Parties

To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements shall require Relying Parties to indemnify VeriSign and any non-VeriSign CAs or RAs for:

- The Relying Party's failure to perform the obligations of a Relying Party,
- The Relying Party's reliance on a Certificate that is not reasonable under the circumstances, or
- The Relying Party's failure to check the status of such Certificate to determine if the Certificate is expired or revoked.

2.3.2 Fiduciary Relationships

To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements shall disclaim any fiduciary relationship between VeriSign or a non-VeriSign CA or RA on one hand and a Subscriber or Relying Party on the other hand.

2.3.3 Administrative Processes

VeriSign, Affiliates, Managed PKI Customers, and Gateway Customers shall have sufficient financial resources to maintain their operations and perform their duties, and they must be reasonably able to bear the risk of liability to Subscribers and Relying Parties. VeriSign, Affiliates, Managed PKI Customers, and Gateway Customers shall also maintain a commercially reasonable level of insurance coverage for errors and omissions, either through an errors and omissions insurance program with an insurance carrier or a self-insured retention. This insurance requirement does not apply to governmental entities.

2.4 Interpretation and Enforcement (Class 1-3)

2.4.1 Governing Law

Subject to any limits appearing in applicable law, the laws of the state of California, U.S.A., shall govern the enforceability, construction, interpretation, and validity of this CP, irrespective of contract or other choice of law provisions and without the requirement to establish a commercial nexus in California, USA. This choice of law is made to ensure uniform procedures and interpretation for all VTN Participants, no matter where they are located.

This governing law provision applies only to this CP. Agreements incorporating the CP by reference may have their own governing law provisions, provided that this CP § 2.4.1 governs the enforceability, construction, interpretation, and validity of the terms of the CP separate and apart from the remaining provisions of any such agreements, subject to any limitations appearing in 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.

2.4.2 Severability, Survival, Merger, Notice

To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements shall contain severability, survival, merger, and notice clauses. A severability clause in an agreement prevents any determination of the invalidity or unenforceability of a clause in the agreement from impairing the remainder of the agreement. A survival clause specifies the provisions of an agreement that continue in effect despite the termination or expiration of the agreement. A merger clause states that all understandings concerning the subject matter of an agreement are incorporated in the agreement. A notice clause in an agreement sets forth how the parties are to provide notices to each other.

2.4.3 Dispute Resolution Procedures

2.4.3.1 Disputes Among VeriSign, Affiliates, and Customers

Disputes among one or more of any of VeriSign, Affiliates, or Customers shall be resolved pursuant to provisions in the applicable agreements among the parties.

2.4.3.2 Disputes with End-User Subscribers or Relying Parties

To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements shall contain a dispute resolution clause. The procedures in the Affiliate Practices Legal Requirements Guidebook to resolve disputes involving VeriSign require an initial negotiation period of sixty (60) days followed by litigation in the federal or state court encompassing Santa Clara County, California, in the case of claimants who are U.S. residents, or, in the case of all other claimants, arbitration administered by the International Chamber of Commerce (“ICC”) in accordance with the ICC Rules of Conciliation and Arbitration.

2.5 Fees (Class 1-3)

2.5.1 Certificate Issuance or Renewal Fees

VeriSign, Affiliates, and Customers are entitled to charge end-user Subscribers for the issuance, management, and renewal of Certificates.

2.5.2 Certificate Access Fees

VeriSign, Affiliates, and Customers shall not charge a fee as a condition of making a Certificate available in a repository or otherwise making Certificates available to Relying Parties.

2.5.3 Revocation or Status Information Access Fees

VeriSign and Affiliates shall not charge a fee as a condition of making the CRLs required by CP § 4.4.9 available in a repository or otherwise available to Relying Parties. They shall, however, be entitled to charge a fee for providing customized CRLs, OCSP services, or other value-added revocation and status information services. VeriSign and Affiliates shall not permit access to revocation information, Certificate status information, or time stamping in their repositories by third parties that provide products or services that utilize such Certificate status information without VeriSign’s prior express written consent.

2.5.4 Fees for Other Services Such as Policy Information

VeriSign and Affiliates shall not charge a fee for access to this CP or their respective CPSs. Any use made for purposes other than simply viewing the document, such as reproduction, redistribution, modification, or creation of derivative works, shall be subject to a license agreement with the entity holding the copyright to the document.

2.5.5 Refund Policy

To the extent permitted by applicable law, VeriSign, Affiliates, Universal Service Centers, and those Resellers using Subscriber Agreements shall implement a refund policy in accordance with the Affiliate Practices Legal Requirements Guidebook (in the case of VeriSign and Affiliates) or the requirements of VeriSign or the Affiliate (in the case of Universal Service Centers and Resellers). They shall place their refund policies within their web sites (including a listing in their repositories), in their Subscriber Agreements, and, in the case of VeriSign and Affiliates, in their CPSs.

2.6 Publication and Repository (Class 1-3)

2.6.1 Publication of CA Information

2.6.1.1 Publication by VeriSign and Affiliates

VeriSign and Affiliates shall be responsible for repository functions. Processing Centers, as part of their contracts with Service Centers, shall publish Certificates in the Service Center's repository based on Certificate Applications approved by the Service Centers and their Managed PKI Customers, as well as revocation information concerning such Certificates. Managed PKI Lite Customers, Managed PKI for SSL Customers, and Managed PKI for SSL Premium Edition Customers are not required to publish such Certificates or revocation information in a repository, since VeriSign or an Affiliate would be responsible for performing their repository functions.

VeriSign's and Affiliates' CPSs, Subscriber Agreements, and Relying Party Agreements and a link to this CP shall appear in their respective repositories on their web sites. VeriSign and each Affiliate shall publish the URL of the applicable Relying Party Agreement within each Certificate it issues in accordance with CP §§ 3.1.1, 7.1.6, 7.1.8.

Processing Centers shall publish the Certificates they issue on behalf of their own CAs, and the CAs of Client Service Centers, Managed PKI Customers, and ASB Customers in their Subdomain. Upon revocation of an end-user Subscriber's Certificate, the Processing Center that issued the Certificate shall publish notice of such revocation in the repository required by CP § 2.1.5. In addition, Processing Centers shall issue CRLs and, if available, provide OCSP services for their own CAs and the CAs of Service Centers, Managed PKI Customers, Gateway Customers, and ASB Customers within their respective Subdomains, pursuant to CP §§ 4.4.9, 4.4.11. When Gateway Customers provide notice to VeriSign or an Affiliate of a revocation under CP § 2.6.1.2, the applicable Processing Center shall include notice of the revocation in the appropriate repository.

2.6.1.2 Publication by Gateway Customers

Gateway Customers shall publish the Certificates they issue, in accordance with CP § 2.1.5, and to provide Certificate status information. Upon revocation of an end-user Subscriber's Certificate, Gateway Customers shall notify its Superior Entity (either VeriSign or an Affiliate) of the revocation for inclusion in the Superior Entity's repository.

2.6.2 Frequency of Publication

CA information shall be published promptly after it is made available to the CA. CPSs shall contain provisions relating to amendments made to them, and CPS changes shall be published in accordance with such provisions. CP §§ 4.4.9, 4.4.11 govern the frequency of the publication of Certificate status information.

2.6.3 Access Controls

VeriSign and Affiliates shall not intentionally use technical means of limiting access to this CP, the CPS, Certificates, Certificate status information, or CRLs. VeriSign and Affiliates shall,

however, require persons to agree to a Relying Party Agreement or CRL Usage Agreement as a condition to accessing Certificates, Certificate status information, or CRLs. VeriSign and Affiliates shall implement controls to prevent unauthorized persons from adding, deleting, or modifying repository entries.

2.6.4 Repositories

See CP § 2.1.5.

2.7 Compliance Audit

VeriSign, Affiliates, and Customers shall undergo a periodic compliance audit (“Compliance Audit”) to ensure compliance with VTN Standards after they begin operations. The compliance audit requirements appear within the subsections of this CP § 2.7.

In addition to compliance audits, VeriSign and Affiliates shall be entitled to perform other reviews and investigations to ensure the trustworthiness of the VTN, which include, but are not limited to:

- A “Security and Practices Review” of an Affiliate before it is permitted to begin operations. A Security and Practices Review consists of a review of an Affiliate’s secure facility, security document, CPS, VTN-related agreements, privacy policy, and validation plans to ensure that the Affiliate meets VTN Standards.
- VeriSign shall be entitled, within its sole and exclusive discretion, to perform at any time an “Exigent Audit/Investigation” on itself, an Affiliate, or a Customer in the event VeriSign or the Superior Entity of the entity to be audited has reason to believe that the audited entity has failed to meet VTN Standards, has experienced an incident or Compromise, or has acted or failed to act, such that the audited entity’s failure, the incident or Compromise, or the act or failure to act poses an actual or potential threat to the security or integrity of the VTN.
- VeriSign shall be entitled to perform “Supplemental Risk Management Reviews” on itself, an Affiliate, or a Customer following incomplete or exceptional findings in a Compliance Audit or as part of the overall risk management process in the ordinary course of business.

VeriSign shall be entitled to delegate the performance of these audits, reviews, and investigations to the Superior Entity of the entity being audited, reviewed, or investigated or to a third party audit firm. Entities that are subject to an audit, review, or investigation shall provide reasonable cooperation with VeriSign and the personnel performing the audit, review, or investigation.

2.7.1 Frequency of Entity Compliance Audit (Class 1-3)

Compliance Audits shall be conducted at least annually at the sole expense of the audited entity.

2.7.2 Identity/ Qualifications of Auditor

A third party auditing firm shall perform the Compliance Audits of VeriSign, an Affiliate, and Managed PKI Customers approving one hundred (100) or more Class 3 Certificate Applications within a twelve (12) month period. Compliance Audits of Gateway Customers (Class 1) or other

Managed PKI Customers approving Class 1 or 2 Certificate Applications or fewer than one hundred (100) Class 3 Certificate Applications may be self-audits, subject to the limitations in CP § 2.7.2.1.

2.7.2.1 Personnel Performing Self-Audits (Class 1-3)

Compliance Audits that are self-audits of Gateway Customers or Managed PKI Customers approving Class 1 or 2 Certificate Applications or approving fewer than one hundred (100) Class 3 Certificate Applications shall be performed by a person within the audited entity that is organizationally independent of the Gateway Administrator, Managed PKI Administrator, Key Manager Administrator, or other Administrators performing CA/RA functions. VeriSign recommends that the audit be completed by the entity's internal audit department if one exists.

If the audited entity does not employ a person organizationally independent of such Administrator with the appropriate skills to complete an audit, the audited entity shall employ a qualified independent auditor having the qualifications set forth in CP § 2.7.2.2 to perform the entity's Compliance Audit instead of performing a self-audit. Alternatively, the audited entity may, with VeriSign's or the Superior Entity's advance written consent, utilize a person to perform the audit who is not independent of such audit functions if the audited entity has issued or approved the Certificate Applications for fewer than one hundred (100) Certificates of any Class within the previous twelve (12) months and the entity's Superior Entity and VeriSign have no reason to believe that there have been any security irregularities or incidents within the previous twelve (12) months that have posed an actual or potential threat to the security of the VTN.

2.7.2.2 Qualifications of Third-Party Audit Firms (Class 1-3)

Reviews and audits performed by a third party audit firm shall be performed by a certified public accounting firm with demonstrated expertise in computer security or by accredited computer security professionals employed by a competent security consultancy. Such firm shall also have demonstrated expertise in the performance of IT security and PKI compliance audits.

2.7.3 Auditor's Relationship to Audited Party (Class 1-3)

Compliance Audits performed by third-party audit firms shall be conducted by firms independent of the audited entity. Such firms shall not have a conflict of interest that hinders their ability to perform auditing services. With respect to self-audits, see CP § 2.7.2.1.

2.7.4 Topics Covered by Audit

Audit topics for each category of entity are set forth below. The audited entity may make a Compliance Audit a module that is part of an overall annual audit of the entity's information systems.

2.7.4.1 Self-Audits of Gateway Customers (Class 1)

An audit program guide describes the procedures for auditing Gateway Customers. Gateway Customers shall meet their annual Compliance Audit requirement via a self-audit attesting to the

satisfaction of the control objectives in the audit program guide and noting any exceptions or irregularities.

2.7.4.2 Self-Audits of Managed PKI Customers (Class 1-2)

An audit program guide describes the procedures for auditing Managed PKI Customers that approve Class 1 and 2 Certificate Applications. Such Managed PKI Customers shall meet their annual Compliance Audit requirement via a self-audit attesting to the satisfaction of the control objectives in the audit program guide and noting any exceptions or irregularities.

2.7.4.3 Audit of an Managed PKI Customer (Class 3)

An audit program guide describes the procedures for auditing Managed PKI Customers that approve Class 3 Certificate Applications. If such Managed PKI Customers approve one hundred (100) or more Class 3 Certificate Applications within a twelve (12) month period, such Managed PKI Customers shall meet their annual Compliance Audit requirement via an audit by a third-party auditing firm attesting to the satisfaction of the control objectives in the audit program guide and noting any exceptions or irregularities. If not, such Managed PKI Customers shall meet their annual Compliance Audit requirement via a self-audit attesting to the satisfaction of the control objectives in the audit program guide and noting any exceptions or irregularities.

2.7.4.4 Audit of VeriSign or an Affiliate (Class 1-3)

VeriSign and each Affiliate shall be audited pursuant to the Affiliate Audit Program Guide, which incorporates guidelines provided in the American Institute of Certificate Public Accounts' Statement on Auditing Standards (SAS) Number 70, *Reports on the Processing of Transactions by Service Organizations*. Their Compliance Audits shall be a SAS 70 Type II Review: A Report of Policies and Procedures in Operation and Test of Operational Effectiveness, or an equivalent audit standard approved by VeriSign.

2.7.5 Actions Taken as a Result of Deficiency (Class 1-3)

After receiving a report based on the Compliance Audit under CP § 2.7.6, the audited entity's Superior Entity shall contact the audited party to discuss any exceptions or deficiencies shown by the Compliance Audit. VeriSign shall also be entitled to discuss such exceptions or deficiencies with the audited party. The audited entity and the Superior Entity shall, in good faith, use commercially reasonable efforts to agree on a corrective action plan for correcting the problems causing the exceptions or deficiencies and to implement the plan. The audited entity's failure to develop such a corrective action plan or implement it, or if the report reveals exceptions or deficiencies that VeriSign and the audited entity's Superior Entity reasonably believe pose an immediate threat to the security or integrity of the VTN, (a) VeriSign and/or the Superior Entity shall determine whether revocation and Compromise reporting are necessary under CP §§ 4.4.1.1, 4.4.15, (b) VeriSign and the Superior Entity shall be entitled to suspend services to the audited entity, and (c) if necessary, VeriSign and the Superior Entity may terminate such services subject to CP § 4.9 and the terms of the audited entity's contract with its Superior Entity

2.7.6 Communications of Results (Class 1-3)

Following any Compliance Audit, the audited entity shall provide VeriSign and its Superior Entity (if the Superior Entity is not VeriSign) with the annual report and attestations based on its audit or self-audit within fourteen (14) days after the completion of the audit and no later than forty-five (45) days after the anniversary date of commencement of operations.

2.8 Confidentiality and Privacy (Class 1-3)

VeriSign and Affiliates shall implement a privacy policy in accordance with the Affiliate Practices Legal Requirements Guidebook. Such privacy policies shall conform to applicable local privacy laws. VeriSign and Affiliates shall not disclose or sell the names of Certificate Applicants or other identifying information about them, subject to CP § 2.8.2 and to right of a terminating CA to transfer such information to a successor CA under CP § 4.9.

2.8.1 Types of Information to be Kept Confidential and Private

The following records of Subscribers shall, subject to CP § 2.8.2, be kept confidential and private (“Confidential/Private Information”):

- CA application records, whether approved or disapproved,
- Certificate Application records (subject to CP § 2.8.2),
- Private keys held by Managed PKI Customers using Managed PKI Key Manager and information needed to recover such Private Keys,
- Transactional records (both full records and the audit trail of transactions),
- VTN audit trail records created or retained by VeriSign, an Affiliate, or a Customer,
- VTN audit reports created by VeriSign, an Affiliate, or a Customer (to the extent such reports are maintained), or their respective auditors (whether internal or public),
- Contingency planning and disaster recovery plans, and
- Security measures controlling the operations of VeriSign or Affiliate hardware and software and the administration of Certificate services and designated enrollment services.

2.8.2 Types of Information Not Considered Confidential or Private

VTN Participants acknowledge that Certificates, Certificate revocation and other status information, repositories of VTN Participants, and information contained within them are not considered Confidential/Private Information. Information not expressly deemed Confidential/Private Information under CP § 2.8.1 shall be considered neither confidential nor private. This section is subject to applicable privacy laws.

2.8.3 Disclosure of Certificate Revocation/Suspension Information

See CP § 2.8.2.

2.8.4 Release to Law Enforcement Officials

VTN Participants acknowledge that VeriSign and the Affiliate shall be entitled to disclose Confidential/Private Information if, in good faith, VeriSign or the Affiliate believes disclosure is necessary in response to subpoenas and search warrants. This section is subject to applicable privacy laws.

2.8.5 Release as Part of Civil Discovery

VTN Participants acknowledge that VeriSign and the Affiliate shall be entitled to disclose Confidential/Private Information if, in good faith, the Affiliate or VeriSign believes disclosure is necessary in response to judicial, administrative, or other legal process during the discovery process in a civil or administrative action, such as subpoenas, interrogatories, requests for admission, and requests for production of documents. This section is subject to applicable privacy laws.

2.8.6 Disclosure Upon Owner's Request

Privacy policies established pursuant to CP § 2.8 shall contain provisions relating to the disclosure of Confidential/Private Information to the person disclosing it to VeriSign or the Affiliate. This section is subject to applicable privacy laws.

2.8.7 Other Information Release Circumstances

No stipulation.

2.9 Intellectual Property Rights (Class 1-3)

The allocation of Intellectual Property Rights among VTN Participants other than Subscribers and Relying Parties shall be governed by the applicable agreements among such VTN Participants. The following subsections of CP § 2.9 apply to the Intellectual Property Rights in relation to Subscribers and Relying Parties.

2.9.1 Property Rights in Certificates and Revocation Information

CAs retain all Intellectual Property Rights in and to the Certificates and revocation information that they issue. VeriSign, Affiliates, and Customers shall grant permission to reproduce and distribute Certificates on a nonexclusive royalty-free basis, provided that they are reproduced in full and that use of Certificates is subject to the Relying Party Agreement referenced in the Certificate. VeriSign, Affiliates, and Customers shall grant permission to use revocation information to perform Relying Party functions subject to the applicable CRL Usage Agreement, Relying Party Agreement, or any other applicable agreements.

2.9.2 Property Rights in the CP

VTN Participants acknowledge that VeriSign retains all Intellectual Property Rights in and to this CP.

2.9.3 Property Rights in Names

A Certificate Applicant retains all rights it has (if any) in any trademark, service mark, or trade name contained in any Certificate Application and distinguished name within any Certificate issued to such Certificate Applicant.

2.9.4 Property Rights in Keys and Key Material

Key pairs corresponding to Certificates of CAs and end-user Subscribers are the property of the CAs and end-user Subscribers that are the respective Subjects of these Certificates, subject to the rights of Managed PKI Customers using Managed PKI Key Manager, regardless of the physical medium within which they are stored and protected, and such persons retain all Intellectual Property Rights in and to these key pairs. Without limiting the generality of the foregoing, VeriSign's root public keys and the root Certificates containing them, including all PCA public keys and self-signed Certificates, are the property of VeriSign. VeriSign licenses software and hardware manufacturers to reproduce such root Certificates to place copies in trustworthy hardware devices or software. Finally, without limiting the generality of the foregoing, Secret Shares of a CA's private key are the property of the CA, and the CA retains all Intellectual Property Right in and to such Secret Shares even though they cannot obtain physical possession of the those shares or the CA from VeriSign.

3. Identification and Authentication

3.1 Initial Registration

3.1.1 Types of Names (Class 1-3)

End-user Subscriber Certificates shall contain an X.501 distinguished name in the Subject name field. The Subject distinguished name of end-user Subscriber Certificates shall include a common name (CN=) component. The authenticated common name value included in the Subject distinguished names of organizational Certificates shall be a domain name (in the case of Secure Server IDs and Global Server IDs) or the legal name of the organization or unit within the organization. The authenticated common name value included in the Subject distinguished name of a Class 3 Organizational ASB Certificate, however, shall be the generally accepted personal name of the organizational representative authorized to use the organization's private key, and the organization (O=) component shall be the legal name of the organization. The common name value included in the Subject distinguished name of individual Certificates shall represent the individual's generally accepted personal name. Common names shall be authenticated in the case of Class 2-3 Certificates. VTN Certificates shall contain a reference to the applicable Relying Party Agreement in their distinguished names, in accordance with CP § 7.1.4.

3.1.2 Need for Names to be Meaningful (Class 1-3)

Class 2 and 3 end-user Subscriber Certificates shall include meaningful names in the following sense: Class 2 and 3 end-user Subscriber Certificates shall contain names with commonly understood semantics permitting the determination of the identity of the individual or

organization that is the Subject of the Certificate. For such Certificates, pseudonyms (names other than a Subscriber's true personal or organizational name) shall not be permitted.

3.1.3 Rules for Interpreting Various Name Forms (Class 1-3)

No stipulation.

3.1.4 Uniqueness of Names (Class 1-3)

The names of Subscribers within the VTN shall be unique within an Affiliate's and Customer's Subdomains for a specific class of Certificate. It is possible for a Subscriber to have two or more certificates with the same Subject Distinguished Name.

3.1.5 Name Claim Dispute Resolution Procedure (Class 1-3)

Certificate Applicants shall not use names in their Certificate Applications that infringe upon the Intellectual Property Rights of others. Neither VeriSign nor any Affiliate shall be required to determine whether a Certificate Applicant has Intellectual Property Rights in the name appearing in a Certificate Application or to arbitrate, mediate, or otherwise resolve any dispute concerning the ownership of any domain name, trade name, trademark, or service mark, and VeriSign and any Affiliate shall be entitled, without liability to any Certificate Applicant, to reject or suspend any Certificate Application because of such dispute.

3.1.6 Recognition, Authentication, and Role of Trademarks (Class 1-3)

See CP § 3.1.5.

3.1.7 Method to Prove Possession of Private Key (Class 1-3)

The method to prove possession of a private key shall be PKCS #10, another cryptographically-equivalent demonstration, or another VeriSign-approved method. This requirement does not apply where a key pair is generated by a CA on behalf of a Subscriber, for example where pre-generated keys are placed on smart cards.

3.1.8 Authentication of Organization Identity

3.1.8.1 Authentication of the Identity of Organizational End-User Subscribers (Class 3)

The identity of organizational end-user Subscribers and other enrollment information provided by Certificate Applicants (except for Nonverified Subscriber Information) shall be confirmed in accordance with the procedures set forth in VeriSign's documented Validation Procedures. Affiliates' procedures for the authentication of organizational identity shall be submitted to VeriSign for approval, and such approval shall be a condition of an Affiliate beginning its operations as CA or RA to approve Certificate Applications for or issue Class 3 organizational Certificates. In addition to the procedures below, the Certificate Applicant must demonstrate that it rightfully holds the private key corresponding to the public key to be listed in the Certificate in accordance with CP § 3.1.7.

3.1.8.1.1 Authentication for Retail Organizational Certificates

Confirmation of the identity of a Certificate Applicant for a Retail organizational Certificate shall include:

- A determination that the organization exists by using at least one third party identity proofing service or database, or alternatively, organizational documentation issued by or filed with the applicable government that confirms the existence of the organization,
- In the case of server Certificates, a determination that the Certificate Applicant is the record owner of the domain name of the server that is the Subject of the Certificate or is otherwise authorized to use the domain,
- A confirmation by telephone, confirmatory postal mail, or comparable procedure to the Certificate Applicant to confirm certain information about the organization, confirm that the organization has authorized the Certificate Application, and confirm that the person submitting the Certificate Application on behalf of the Certificate Applicant is authorized to do so, and
- In the case of Global Server IDs, the additional checks necessary to satisfy United States export regulations and licenses issued by the United States Department of Commerce Bureau of Industry and Science (“BIS”) (formerly known as the Bureau of Export Administration (“BXA”).

3.1.8.1.2 Authentication for Managed PKI for SSL or Managed PKI for SSL Premium Edition

With respect to Managed PKI for SSL Customers and Managed PKI for SSL Premium Edition Customers, the identity confirmation process begins with VeriSign’s or an Affiliate’s confirmation of the identity of the Managed PKI for SSL Customer or Managed PKI for SSL Premium Edition Customer itself in accordance with CP § 3.1.8.2. Following such confirmation, the Managed PKI for SSL Customer or Managed PKI for SSL Premium Edition Customer is responsible for approving the issuance of Certificates to servers within its own organization by:

- Ensuring that the server designated as the Subject of a Secure Server ID or Global Server ID actually exists, and
- Ensuring the organization has authorized the issuance of a Secure Server ID or Global Server ID to the server.

3.1.8.1.3 Authentication for Class 3 Organizational ASB Certificates

Confirmation of the identity of a Certificate Applicant for a Class 3 Organizational ASB Certificate shall include:

- A determination that the organization exists by using at least one third party identity proofing service or database, or alternatively, organizational documentation issued by or filed with the applicable government that confirms the existence of the organization,
- A confirmation by telephone, confirmatory postal mail, and/or comparable procedure to the Certificate Applicant to confirm certain information about the organization, confirm that the organization has authorized the Certificate Application, confirm the employment of the representative submitting the Certificate Application on behalf of the Certificate Applicant, and confirm the authority of the representative to act on behalf of the Certificate Applicant, and

- A confirmation by telephone, confirmatory postal mail, and/or comparable procedure to the Certificate Applicant’s representative to confirm that the person named as representative has submitted the Certificate Application.

3.1.8.2 Authentication of the Identity of CAs and RAs (Class 1-3)

Affiliates, Managed PKI Customers, Gateway Customers, and ASB Customers, before becoming CAs or RAs, enter into an agreement with an entity above it within the Class 1, 2, or 3 VTN hierarchy (the “Superior Entity”) or a Universal Service Center or Reseller marketing on behalf of VeriSign or an Affiliate. The table below shows the possible Superior Entities corresponding to each CA Certificate Applicant.

<i>CA or RA</i>	<i>Superior Entity</i>
Processing Center	VeriSign
Service Center	Processing Center
Managed PKI Customer or Gateway Customer	Processing Center or Service Center
ASB Customer	ASB Provider

Table 6 – CAs and RAs and Their Superior Entities

The Superior Entity shall authenticate the identity of the prospective Affiliate, Managed PKI Customer, Gateway Customer, or ASB Customer before final approval of its status as CA or RA, except where VeriSign or an Affiliate delegates such responsibility to a Universal Service Center or Reseller. Where such delegation has occurred, the Universal Service Center or Reseller shall authenticate the identity of the prospective Managed PKI Customer. For purposes of the CP, however, VeriSign or the Affiliate remains the Superior Entity, rather than the Universal Service Center or Reseller. Affiliates’ procedures for the authentication of the organizational identity of Managed PKI Customers, Gateway Customers, and ASB Customers shall be submitted to VeriSign for approval, and such approval is a condition of an Affiliate beginning its operations as a provider of Managed PKI , Gateway, or Authentication Service Bureau services, as the case may be. Universal Service Centers’ and Resellers’ procedures for such authentication of organizational identity shall be submitted to VeriSign or the applicable Affiliate, and such approval is a condition of a Universal Service Center or Reseller beginning its operations as a provider of Managed PKI or Authentication Service Bureau services, as the case may be.

The identity of Affiliates, Managed PKI Customers, Gateway Customers, and ASB Customers shall be confirmed either by:

- The personal appearance of an authorized representative of the organization before authorized personnel of the organization’s Superior Entity, a Universal Service Center, or Reseller, coupled with authorization procedures to ensure the confirmation of the organization and the authority of its personnel, or
- In the case of VeriSign or an Affiliate confirming the identity of Managed PKI Customers, Gateway Customers, and ASB Customers, the procedures set forth in the Affiliate Practices Legal Requirements Guidebook or, in the case of Universal Service Centers or Resellers confirming the identity of Managed PKI Customers or ASB

Customers, the VeriSign or Affiliate requirements placed on Universal Service Centers and Resellers. These procedures include:

- The checks required for the confirmation of the identity of organizational end-user Subscribers under CP § 3.1.8.1, except that instead of a Certificate Application, the validation is of an application to become a Managed PKI Customer, Gateway Customer, or ASB Customer, and
- In the case of Managed PKI Customers or Gateway Customers, confirming that the person identified as Managed PKI Administrator or Gateway Administrator is authorized to act in the capacity.

3.1.9 Authentication of Individual Identity

Authentication procedures shall be in accordance with the specific requirements for each Class of Certificate as set forth in the Affiliate Practices Legal Requirements Guidebook. Stronger methods of authentication for each Class of Certificate than the ones set forth in this Section 3.1.9 shall be permitted in order to meet business needs.

The authentication procedures in common for each Class of Certificate are confirming that the Certificate Applicant is the person identified in the Certificate Application (except for Certificate Applicants for Class 1 Certificates), that the Certificate Applicant rightfully holds the private key corresponding to the public key to be listed in the Certificate in accordance with CP § 3.1.7, and that the information to be listed in the Certificate is accurate, except for Nonverified Subscriber Information. These procedures are in addition to the more detailed procedures described below for each Class of Certificate.

Affiliates' procedures for the authentication of individual identity shall be approved by VeriSign prior to an Affiliate beginning its operations as CA or RA to issue or approve Certificate Applications for Class 1-3 individual Certificates or as a provider of services to Customers issuing or approving Certificate Applications for Class 1-3 individual Certificates.

3.1.9.1 Class 1 Certificates

Authentication of individuals for Class 1 Certificates shall consist of a check to ensure that the Subject distinguished name is a unique and unambiguous Subject name within the VeriSign, an Affiliate's, or a Gateway Customer's Class 1 Subdomain. Class 1 authentication does not provide assurances of identity, i.e., that a Subscriber is who he or she claims to be. The common name of the Subscriber is Nonverified Subscriber Information. Class 1 authentication also includes a limited confirmation of the Certificate Applicant's e-mail address. Service Centers offering Class 1 Certificates delegate these authentication functions to a Processing Center.

Authentication by Managed PKI Customers and Gateway Customers for Class 1 Managed PKI Certificates includes the above authentication procedures, which are also delegated to their Superior Entities and ultimately to a Processing Center. In addition, however, the Managed PKI Customer or Gateway Customer must determine that the Certificate Applicant is an Affiliated Individual in relation to the Managed PKI Customer or Gateway Customer before approving the Certificate Application.

3.1.9.2 Class 2 Certificates

Authentication of Class 2 Certificate Applications takes place in one of two ways. First, for Managed PKI Certificates, Managed PKI Customers and Managed PKI Lite Customers use business records or databases of business information to approve or deny Certificate Applications pursuant to CP § 3.1.9.2.1. A second method of authentication, which applies to Retail Class 2 Certificates and Class 2 Individual ASB Certificates, requires VeriSign or an Affiliate to confirm the identity of Certificate Applications using information residing in the database of a VeriSign-approved identity proofing service under CP § 3.1.9.2.2.

3.1.9.2.1 Class 2 Managed PKI Certificates

Managed PKI Customers and Managed PKI Lite Customers shall confirm the identity of individuals by comparing enrollment information against their own business records or databases of business information. For example, they may check enrollment information against employee or independent contractor records in a human resources department database. The Managed PKI Customer or Managed PKI Lite Customer may approve the Certificate Application manually using the Managed PKI Control Center if the enrollment information matches the records or database used for authentication. This process is known as “Manual Authentication.”

Managed PKI’s Automated Administration Software Module and other similar VTN software give Managed PKI Customers the option of automatic approval and revocation of users or devices directly from pre-existing administrative systems or databases, rather than requiring Manual Authentication for each Certificate Application. Managed PKI Customers using the Managed PKI Automated Administration Software Module authenticate the identity of potential Certificate Applications before placing their information in a database. When a Certificate Applicant submits a Certificate Application, then, the Automated Administration Software Module compares information in the Certificate Application with the database and, if the information matches, automatically approves the Certificate Application for immediate issuance by the Processing Center. This process is called “Automated Administration.” Managed PKI Customers not using Automated Administration or similar VTN software, as well as Managed PKI Lite Customers, must use Manual Authentication.

3.1.9.2.2 Class 2 Retail Certificates

VeriSign and Affiliates shall validate Certificate Applications for Class 2 Retail Certificates and Class 2 Individual ASB Certificates by determining if identifying information in the Certificate Application matches information residing in the database of a VeriSign-approved identity proofing service, such as a major credit bureau or other reliable source of information providing services in VeriSign’s or the Affiliate’s country or territory. If the information in the Certificate Application matches the information in the database, the Affiliate may approve the Certificate Application.

3.1.9.3 Class 3 Individual Certificates

The authentication of Class 3 individual Certificates is based on the personal (physical) presence of the Certificate Applicant before an agent of the Affiliate or Managed PKI Customer, or before a notary public or other official with comparable authority within the Certificate Applicant’s

jurisdiction. The agent, notary or other official shall check the identity of the Certificate Applicant against a well-recognized form of government-issued identification, such as a passport or driver's license and one other identification credential.

The authentication of Administrators for Class 3 Administrator Certificates shall consist of authenticating the existence of the Administrator's employer (an Affiliate or Managed PKI Customer) and confirming the employment and authorization of the person named as Administrator. VeriSign and Affiliates shall authenticate Certificate Applications first by authenticating the identity of the entity employing or retaining the Administrator pursuant to CP § 3.1.8.2. Such entity shall either be a Processing Center, Service Center, or Managed PKI Customer. VeriSign and Affiliates shall also, during such authentication process, confirm the authorization of the Certificate Applicant to act as Administrator.

VeriSign and Affiliate may also have occasion to approve Certificate Applications for their own Administrators. Administrators are "Trusted Persons" within an organization (see CP § 5.2.1). In this case, authentication of their Certificate Applications shall be based on confirmation of their identity in connection with their employment or retention as an independent contractor (see CP § 5.2.3) and background checking procedures (see CP § 5.3.2).

VeriSign and Affiliate may approve Administrator Certificates to be associated with a non-human recipient such as a device, or a server. Authentication of a Class 3 Administrator Certificate Applications for a non-human recipient shall include:

- Authentication of the existence and identity of the service named as the Administrator in the Certificate Application
- Authentication that the service has been securely implemented in a manner consistent with it performing an Administrative function
- Confirmation of the employment and authorization of the person enrolling for the Administrator certificate for the service named as Administrator in the Certificate Application.

3.2 Routine Rekey (Renewal) (Class 1-3)

3.2.1 Renewal of End-User Subscriber Certificates

The entity approving a Certificate Application for the Subscriber of an end-user Subscriber Certificate shall be responsible for authenticating a request for renewal. Renewal procedures shall ensure that the person or organization seeking to renew an end-user Subscriber Certificate is in fact the Subscriber of the Certificate.

One acceptable procedure is through the use of a Challenge Phrase (or the equivalent thereof), or proof of possession of the private key. Subscribers choose and submit with their enrollment information a Challenge Phrase. Upon renewal of a Certificate, if a Subscriber correctly submits the Subscriber's Challenge Phrase (or the equivalent thereof) with the Subscriber's reenrollment information, and the enrollment information (including contact information) has not changed, a renewal Certificate is automatically issued. After rekeying or renewal in this fashion, and on at least alternative instances of subsequent rekeying or renewal thereafter, the CA or RA shall

reconfirm the identity of the Subscriber in accordance with the requirements specified in its CP §§ 3.1.8.1, 3.1.9 for the authentication of an original Certificate Application.

Other than this procedure or another VeriSign-approved procedure, the requirements for the authentication of an original Certificate Application in CP §§ 3.1.8.1, 3.1.9 shall be used for renewing an end-user Subscriber Certificate. The authentication of a request to renew a Class 3 Organizational ASB Certificate, however, requires the use of a Challenge Phrase as well as the authentication procedures for an original Certificate Application under CP § 3.1.8.1.3.

3.2.2 Renewal of CA Certificates

A CA's Superior Entity approving an application for a CA Certificate shall be responsible for authenticating a request for renewal. Renewal procedures shall ensure that an organization seeking to renew the CA Certificate of a Processing Center, Client Service Center, Managed PKI Customer, Gateway Customer, or ASB Customer is in fact the Subscriber of the CA Certificate. Authentication procedures shall be the same as original enrollment pursuant to CP § 3.1.8.2.

3.3 Rekey After Revocation (Class 1-3)

Renewal after revocation is governed by this CP § 3.3. Renewal after revocation shall not be permitted, however, if revocation occurred because the Certificate (other than a Class 1 Certificate) was issued to a person other than the one named as the Subject of the Certificate, or the Certificate (other than a Class 1 Certificate) was issued without the authorization of the person named as the Subject of such Certificate, or the entity approving the Subscriber's Certificate Application discovers or has reason to believe that a material fact in the Certificate Application is false.

Subject to the foregoing paragraph, renewal of an organizational or CA Certificate following revocation of the Certificate is permissible as long as renewal procedures ensure that the organization or CA seeking renewal is in fact the Subscriber of the Certificate. Renewed organizational Certificates shall contain the same Subject distinguished name as the Subject distinguished name of the organizational Certificate being renewed.

Renewal of an individual Certificate following revocation again must ensure that the person seeking renewal is, in fact, the Subscriber. One acceptable procedure is the use of a Challenge Phrase (or the equivalent thereof), as described in CP § 3.2.1. Other than this procedure or another VeriSign-approved procedure, the requirements for the validation of an original Certificate Application in CP §§ 3.1.8.1, 3.1.9 shall be used for renewing a Certificate following revocation.

3.4 Revocation Request (Class 1-3)

Revocation procedures shall ensure prior to any revocation of any Certificate that the revocation has in fact been requested by the Certificate's Subscriber, the entity that approved the Certificate Application, the applicable Processing Center, or, in the case of Certificates issued by an ASB Customer CA, the applicable ASB Customer. Acceptable procedures for authenticating the revocation requests of a Subscriber include:

- Having the Subscriber for certain certificate types submit the Subscriber's Challenge Phrase (or the equivalent thereof), and revoking the Certificate automatically if it matches the Challenge Phrase (or the equivalent thereof) on record,²
- Receiving a message purporting to be from the Subscriber that requests revocation and contains a digital signature verifiable with reference to the Certificate to be revoked, and
- Communication with the Subscriber providing reasonable assurances in light of the Class of Certificate that the person or organization requesting revocation is, in fact the Subscriber. Such communication, depending on the circumstances, may include one or more of the following: telephone, facsimile, e-mail, postal mail, or courier service.

CA/RA Administrators are entitled to request the revocation of end-user Subscriber Certificates within the CA's/RA's Subdomain. VeriSign and Affiliates shall authenticate the identity of Administrators via access control using SSL and client authentication before permitting them to perform revocation functions. In the case of ASB Customers' CA Administrators providing revocation instructions, however, the ASB Providers shall authenticate the identity of such CA Administrators using telephone communications.

Managed PKI Customers using the Automated Administration Software Module may submit bulk revocation requests to a Processing Center. Such requests shall be authenticated via a digitally signed request signed with the private key in the Managed PKI Customer's Automated Administration hardware token.

The requests of Processing Centers, Client Service Centers, Managed PKI Customers, and Gateway Customers to revoke a CA Certificate shall be authenticated by their Superior Entities to ensure that the revocation has in fact been requested by the CA. Processing Centers receiving a request from a Service Center to revoke, upon the Service Center's own initiative, the CA Certificate of one of the Service Center's Managed PKI Customers or Gateway Customers shall authenticate the request to ensure that the revocation has in fact been requested by the Service Center.

4. Operational Requirements

4.1 Certificate Application (Class 1-3)

4.1.1 Certificate Applications for End-User Subscriber Certificates

All end-user Certificate Applicants shall undergo an enrollment process consisting of:

- completing a Certificate Application and providing the requested information,
- generating, or arranging to have generated, a key pair in accordance with CP § 6.1,
- delivering his, her, or its public key to the issuing Processing Center or Gateway Customer in accordance with CP § 6.1.3,

² **Automatic** Online revocation **using a challenge phrase** is not available for VeriSign Class 3 Code and Content Signing Certificates. These certificates will be revoked and published on the appropriate CRL upon request by the subscriber to VeriSign to revoke the certificate. The request must clearly indicate upon which of the circumstances listed in § 4.4.1.1 the revocation request is based. To request the revocation Subscribers must contact VeriSign customer service: E-mail: support@verisign.com, or Phone: 1-877-438-8776 or 1-650-426-3400. VeriSign will verify the revocation request and reasons for revocation before revoking the certificate.

- demonstrating to the issuing Processing Center or Gateway Customer pursuant to CP § 3.1.7 that the Certificate Applicant has possession of the private key corresponding to the public key delivered to the Processing Center or Gateway Customer, and
- manifesting assent to the relevant Subscriber Agreement.

Web Hosts may submit Certificate Applications on behalf of their customers pursuant to the Web Host Program (see CP § 1.1.2.6).

Certificate Applications are submitted either to a Processing Center, Service Center, Managed PKI Customer, or Gateway Customer for processing and ultimate either approval or denial. The entity processing the Certificate Application and the entity issuing the Certificate pursuant to CP § 4.2 may be two different entities as shown in the following table.

<i>Certificate Class</i>	<i>Entity Processing Certificate Applications</i>	<i>Entity Issuing Certificate</i>
Class 1 individual Retail Certificate	Processing Center or Service Center	Processing Center
Class 1 individual Certificate (Gateway)	Gateway Customer	Gateway Customer
Class 1 individual Managed PKI Certificate	Class 1 Managed PKI Customer	Processing Center
Class 2 individual Retail Certificate	Processing Center or Service Center	Processing Center
Class 2 individual ASB Certificate	ASB Provider (Processing Center or Service Center)	Processing Center
Class 2 individual Managed PKI Certificate	Class 2 Managed PKI Customer or Managed PKI Lite Customer	Processing Center
Class 3 individual Retail Certificate	Processing Center or Service Center	Processing Center
Class 3 Administrator Certificate	Processing Center or Service Center	Processing Center
Class 3 organizational Retail Certificates	VeriSign or Service Center	VeriSign
Class 3 organizational Managed PKI Certificates (Managed PKI for SSL or Managed PKI for SSL Premium Edition)	Class 3 Managed PKI for SSL Customer or Managed PKI for SSL Premium Edition Customer	VeriSign
Class 3 Organizational ASB Certificate	ASB Provider (Processing Center or Service Center)	Processing Center

Table 7 – Entities Receiving Certificate Applications

4.1.2 Certificate Applications for CA or RA Certificates

This CP does not require Affiliates or Customers, which are subscribers of CA or RA Certificates, to complete formal Certificate Applications. Instead, they enter into a contract with

their Superior Entities or the Universal Service Centers or Resellers of their Superior Entities. *See* CP § 3.1.8.2. CA and RA Applicants shall provide their credentials as required by CP § 3.1.8.2 to demonstrate their identity and provide contact information during the contracting process. During this contracting process or, at the latest, prior to the Key Generation Ceremony to create a Processing Center's, Client Service Center's, Managed PKI Customer's, Gateway Customer's, or ASB Customer's key pair, the applicant shall cooperate with its Superior Entity to determine the appropriate distinguished name and the content of the Certificates to be issued by the applicant.

4.2 Certificate Issuance (Class 1-3)

4.2.1 Issuance of End-User Subscriber Certificates

After a Certificate Applicant submits a Certificate Application, the entity receiving the Certificate Application (see CP § 4.1.1) shall confirm or disconfirm the information in the Certificate Application (other than Non-Verified Subscriber Information) pursuant to CP §§ 3.1.8.1, 3.1.9. Upon successful performance of all required authentication procedures pursuant to CP § 3.1, the entity receiving the Certificate Application shall approve the Certificate Application. If authentication is unsuccessful, the entity receiving the Certificate Application shall deny the Certificate Application.

A Certificate shall be created and issued following the approval of a Certificate Application or following receipt of an RA's request to issue the Certificate. Processing Centers and Gateway Customers that receive Certificate Applications themselves shall create and issue to a Certificate Applicant a Certificate based on the information in a Certificate Application following their approval of such Certificate Application. When a Service Center, Managed PKI Customer, or ASB Provider approves a Certificate Application and communicates the approval to its Processing Center, the Processing Center shall create a Certificate and issue it to the Certificate Applicant.

The procedures of this section shall also be used for the issuance of Certificates in connection with the submission of a request to renew the Certificate.

4.2.2 Issuance of CA and RA Certificates

The identity of entities wishing to become Affiliates and Customers shall be authenticated in accordance with CP § 3.1.8.2 and, if approved, issued the Certificates needed to perform their CA or RA functions. Before a contract is entered into with an Affiliate or Customer applicant under CP § 4.1.2, the identity of the potential Affiliate or Customer shall be confirmed based on the credentials it presents. The execution of such a contract indicates the complete and final approval of the application by the Superior Entity. The decision to approve or reject an Affiliate or Customer application shall be solely in the discretion of the Superior Entity (or its Universal Service Center or Reseller). Following such approval, the Superior Entity itself (in the case of a Processing Center) or the Processing Center above it in the VTN (in the case of a Service Center) shall issue the Certificate to the Affiliate or Customer CA or RA in accordance with the Key Ceremony Reference Guide, the Security and Audit Requirements Guide, and CP § 6.1.

4.3 Certificate Acceptance (Class 1-3)

Processing Centers, Client Service Centers, Managed PKI Customers, Gateway Customers, and ASB Providers issuing Certificates to end-user Subscribers shall, either directly or through an RA, notify Subscribers that they have created such Certificates, and provide Subscribers with access to the Certificates by notifying them that their Certificates are available and notifying them of the means for obtaining them. If the Processing Center has not established a procedure to notify end-user Subscribers that it has created a Certificate, that the Certificate is pending, and that the Subscribers may retrieve the Certificate, then the Server Service Centers or Managed PKI Lite Customers approving the Subscribers' Certificate Applications shall do so.

Upon issuance, Certificates shall be made available to end-user Subscribers, either by allowing them to download them from a web site or via a message sent to the Subscriber containing the Certificate. For example, a Processing Center may send the Subscriber a PIN, which the Subscriber enters into an enrollment web page to obtain the Certificate. The Certificate may also be sent to the Subscriber in an e-mail. Downloading a Certificate, or installing a Certificate from a message attaching it constitutes the Subscriber's acceptance of the Certificate.

4.4 Certificate Suspension and Revocation (Class 1-3)

4.4.1 Circumstances for Revocation

4.4.1.1 Circumstances for Revoking End-User Subscriber Certificates

Only in the circumstances listed below, must an end-user Subscriber certificate be revoked by VeriSign, a Processing Center, or Affiliate (or by the Subscriber in accordance with CPS § 3.4) and published on a CRL.

An end-user Subscriber Certificate shall be revoked if:

- The entity approving the Subscriber's Certificate Application or an ASB Customer discovers or has reason to believe that there has been a Compromise of the Subscriber's private key,
- The Subscriber has materially breached a material obligation, representation, or warranty under the applicable Subscriber Agreement,
- The Subscriber Agreement with the Subscriber has been terminated,
- The affiliation between an Managed PKI Customer or an ASB Customer issuing Class 3 Organizational ASB Certificates with a Subscriber is terminated or has otherwise ended,
- The affiliation between an organization that is a Subscriber of a Class 3 Organizational ASB Certificate and the organizational representative controlling the Subscriber's private key is terminated or has otherwise ended,
- The entity approving the Subscriber's Certificate Application or ASB Customer discovers or has reason to believe that the Certificate was issued in a manner not materially in accordance with the procedures required by the applicable CPS, the Certificate (other than a Class 1 Certificate) was issued to a person other than the one named as the Subject of the Certificate, or the Certificate (other than a Class 1 Certificate) was issued without the authorization of the person named as the Subject of such Certificate,

- The entity approving the Subscriber's Certificate Application or ASB Customer discovers or has reason to believe that a material fact in the Certificate Application is false,
- The entity approving the Subscriber's Certificate Application or ASB Customer determines that a material prerequisite to Certificate Issuance was neither satisfied nor waived,
- In the case of Class 3 organizational Certificates, the Subscriber's organization name changes,
- The information within the Certificate, other than Nonverified Subscriber Information, is incorrect or has changed, or
- The Subscriber requests revocation of the Certificate in accordance with CP § 3.4.
- The continued use of that certificate is harmful to the VTN

An Administrator Certificate shall also be revoked if the authority of the Administrator Subscriber of the Certificate to act as Administrator has been terminated or otherwise has ended.

Processing Centers and Gateway Customers revoke the Certificates that they issued based on Certificate Applications that they approved themselves. Processing Centers shall also revoke Certificates in accordance with revocation requests from their Service Centers and from Managed PKI Customers and ASB Customers within their Subdomains. VeriSign, Affiliates, Managed PKI Customers, Gateway Customers, and ASB Customers shall initiate revocation of an end-user Subscriber Certificate when required by this CP § 4.4.1.1. Subscriber Agreements shall require end-user Subscribers to notify the entity, either a CA or RA, that approved the Subscriber's Certificate Application if the Subscriber knows or suspects that a Compromise of the Subscriber's private key has occurred in accordance with the procedures in CP § 4.4.3.1.

4.4.1.2 Circumstances for Revoking CA or RA Certificates

The Certificate issued to a Processing Center, Service Center, Managed PKI Customer, Automated Administration hardware token, or Gateway Customer shall be revoked if:

- The CA's or RA's Superior Entity discovers or has reason to believe that there has been a Compromise of the CA or RA private key,
- The agreement between the CA or RA with its Superior Entity has been terminated,
- The CA's or RA's Superior Entity discovers or has reason to believe that the Certificate was issued in a manner not materially in accordance with the procedures required by the applicable CPS, the Certificate was issued to an entity other than the one named as the Subject of the Certificate, or the Certificate was issued without the authorization of the entity named as the Subject of such Certificate,
- The CA's or RA's Superior Entity determines that a material prerequisite to Certificate issuance was neither satisfied nor waived, or
- The CA requests revocation of the Certificate.
- The continued use of that certificate is harmful to the VTN

Processing Centers shall revoke CA Certificates within their Subdomains when this section requires revocation. Client Service Centers, Managed PKI Customers, Gateway Customers, and

ASB Customers must request revocation from the Processing Center that issued the CA Certificate when revocation is required.

4.4.2 Who Can Request Revocation

4.4.2.1 Who Can Request Revocation of an End-User Subscriber Certificate

Individual Subscribers shall be entitled to request the revocation of their own individual Certificates. In the case of organizational Certificates, a duly authorized representative of the organization shall be entitled to request the revocation of Certificates issued to the organization. A duly authorized representative of VeriSign, an Affiliate, or an Managed PKI Customer whose Administrator received an Administrator Certificate shall be entitled to request the revocation of the Administrator's Certificate. The entity that approved a Subscriber's Certificate Application shall also be entitled to revoke or request the revocation of the Subscriber's Certificate. An ASB Customer shall be entitled to initiate the revocation of Certificates that its CA issued.

4.4.2.2 Who Can Request Revocation of a CA or RA Certificate

Only VeriSign is entitled to request or initiate the revocation of the Certificates issued to its own CAs. Non-VeriSign Processing Centers, Service Centers, Managed PKI Customers, Gateway Customers, and ASB Customers shall be entitled, through their duly authorized representatives, to request the revocation of their own Certificates, and their Superior Entities shall be entitled to request or initiate the revocation of their Certificates.

4.4.3 Procedure for Revocation Request

4.4.3.1 Procedure for Requesting the Revocation of an End-User Subscriber Certificate

An end-user Subscriber requesting revocation shall communicate the request to the entity that approved the Subscriber's Certificate Application (a CA or RA), and such entity shall either revoke the Certificate itself (in the case of Processing Centers or Gateway Customers) or request revocation from the Processing Center that issued the Certificate (in the case of Service Centers or Managed PKI Customers). Communication of such request shall be in accordance with CP § 3.4. A Processing Center, Service Center, Managed PKI Customer, Gateway Customer, or ASB Customer revoking an end-user Subscriber Certificate upon its own initiative shall either revoke the Certificate itself (in the case of Processing Centers or Gateway Customers) or request revocation from the Processing Center that issued the Certificate (in the case of Service Centers or Managed PKI Customers) or from the ASB Provider (in the case of ASB Customers). An ASB Provider revoking an end-user Subscriber Certificate shall either revoke the Certificate itself (in the case of ASB Providers that are also Processing Centers) or request revocation from the Processing Center that issued the Certificate (in the case of ASB Providers that are Service Centers).

4.4.3.2 Procedure for Requesting the Request Revocation of a CA or RA Certificate

A CA or RA requesting revocation shall communicate the request to its Superior Entity. Such Superior Entity shall either revoke the Certificate itself (in the case of Processing Centers) or request revocation from the Processing Center that issued the Certificate (in the case of Service

Centers). A CA's or RA's Superior Entity revoking the CA's or RA's Certificate upon its own initiative shall initiate revocation in the same manner.

4.4.4 Revocation Request Grace Period

Revocation requests shall be submitted as promptly as possible, but no later than within a commercially reasonable time.

4.4.5 Circumstances for Suspension

The VTN does not offer suspension services for end-user Subscriber Certificates.

4.4.6 Who Can Request Suspension

Not applicable.

4.4.7 Procedure for Suspension Request

Not applicable.

4.4.8 Limits on Suspension Period

Not applicable.

4.4.9 CRL Issuance Frequency (If Applicable)

The VTN offers CRLs showing the revocation of VTN Certificates and offers status checking services through the VeriSign Repository and Affiliates' repositories. CRLs for end-user Subscriber Certificates shall be issued at least once per day. CRLs for CA Certificates shall be issued at least quarterly, but also whenever a CA Certificate is revoked. CRLs for Authenticated Content Signing (ACS) root CAs are published annually and also whenever a CA Certificate is revoked. If a Certificate listed in a CRL expires, it may be removed from later-issued CRLs after the Certificate's expiration.

4.4.10 Certificate Revocation List Checking Requirements

Relying Parties shall check the status of Certificates on which they wish to rely. One method by which Relying Parties may check Certificate status is by consulting the most recent CRL from the CA that issued the Certificate on which the Relying Party wishes to rely. Alternatively, Relying Parties may meet this requirement either by checking Certificate status using the applicable web-based repository or by using OCSP (if available). VeriSign and Affiliates shall provide Relying Parties with information on how to find the appropriate CRL, web-based repository, or OCSP responder (where available) to check for revocation status.

4.4.11 On-Line Revocation/Status Checking Availability

Online revocation and other Certificate status information shall be available via a web-based repository and, where offered, OCSP. VeriSign and Affiliates shall have a web-based repository that permits Relying Parties to make online inquiries regarding revocation and other Certificate

status information. A Processing Center, as part of its contract with a Service Center, shall host such a repository on behalf of the Service Center. VeriSign and Affiliates shall provide Relying Parties with information on how to find the appropriate repository to check Certificate status and, if OCSP is available, how to find the right OCSP responder. *See* CP § 4.4.9.

4.4.12 On-Line Revocation Checking Requirements

If a Relying Party does not check the status of a Certificate on which the Relying Party wishes to rely by consulting the most recent relevant CRL, the Relying Party shall check Certificate status by consulting the applicable repository or by requesting Certificate status using the applicable OCSP responder (where OCSP services are available).

4.4.13 Other Forms of Revocation Advertisements Available

No stipulation.

4.4.14 Checking Requirements for Other Forms of Revocation Advertisements

No stipulation.

4.4.15 Special Requirements Regarding Key Compromise

VTN Participants shall be notified of an actual or suspected CA private key Compromise using commercially reasonable efforts. VeriSign and Affiliates shall use commercially reasonable efforts to notify potential Relying Parties if they discover, or have reason to believe, that there has been a Compromise of the private key of one of their own CAs or one of the CAs within their Subdomains.

4.5 Security Audit Procedures

4.5.1 Types of Events Recorded

The types of auditable events that must be recorded by each entity are set forth below. All logs, whether electronic or manual, shall contain the date and time of the event, and the identity of the entity that caused the event.

4.5.1.1 Events Recorded by Processing Centers (Class 1-3)

Processing Centers shall record in audit log files events relating to the security of the CA system such as:

- System start-up and shutdown,
- CA application start-up and shutdown,
- Attempts to create, remove, set passwords or change the system privileges of the privileged users (trusted roles),
- Changes to CA details and/or keys,
- Changes to Certificate creation policies e.g., validity period,
- Login and logoff attempts,
- Unauthorized attempts at network access to the CA system,

- Unauthorized attempts to access system files,
- Generation of a CA's own keys and the keys of subordinate CAs,
- Failed read and write operations on the Certificate and repository,
- Certificate lifecycle management-related events (*e.g.*, Certificate Applications, issuance, revocation, and renewal), and
- Cryptographic module lifecycle management-related events (*e.g.*, receipt, use, deinstallation, and retirement).

Processing Centers shall also collect and consolidate, either electronically or manually, security information not CA system generated such as:

- Key Generation Ceremony and key management databases,
- Physical access logs,
- System configuration changes and maintenance,
- Personnel changes,
- Discrepancy and compromise reports,
- Records of the destruction of media containing key material, activation data, or personal Subscriber information, and
- Possession of activation data for CA private key operations.

4.5.1.2 Events Recorded by Service Centers, Managed PKI Customers (Class 1-3)

Service Centers and Managed PKI Customers shall record in audit log files events relating to the security of their systems such as:

- System start-up and shutdown,
- RA application start-up and shutdown,
- Attempts to create, remove, set passwords or change the system privileges of the privileged users (trusted roles),
- Changes to RA details and/or keys,
- Changes to certificate creation policies *e.g.*, validity period,
- Login and logoff attempts,
- Unauthorized attempts at network access to the CA/RA system,
- Unauthorized attempts to access system files,
- Failed read and write operations on the Certificate and repository,
- Certificate lifecycle management-related events (*e.g.*, approval or denial of Certificate Applications, requests for revocation, or requests for renewal), and
- In the case of Managed PKI Customers using Managed PKI Key Manager, the back-up and recovery of end-user Subscriber private keys.

4.5.1.3 Events Recorded by Gateway Customers (Class 1)

Gateway Customers shall record in audit log files events relating to the security of the CA system such as:

- Attempts to create, remove, set passwords or change the system privileges of the privileged users (trusted roles),
- Changes to CA details and/or keys,

- Unauthorized attempts at network access to the CA system,
- Unauthorized attempts to access system files,
- Generation of CA keys,
- Creation and revocation of certificates,
- Certificate lifecycle management-related events (*e.g.*, Certificate Applications, issuance, revocation, and renewal), and
- Cryptographic module lifecycle management-related events (*e.g.*, receipt, use, deinstallation, and retirement), where a cryptographic module is used.

4.5.2 Frequency of Processing Log (Class 1-3)

Processing Centers, Service Centers, Managed PKI Customers, and Gateway Customers shall review their audit logs in response to alerts based on irregularities and incidents within their CA/RA systems. Processing Centers shall compare their audit logs with the supporting manual and electronic logs from their Managed PKI Customers and Service Centers when any action is deemed suspicious.

Audit log processing shall consist of a review of the audit logs and documenting the reason for all significant events in an audit log summary. Audit log reviews shall include a verification that the log has not been tampered with, an inspection of all log entries, and an investigation of any alerts or irregularities in the logs. Actions taken based on audit log reviews shall be documented.

4.5.3 Retention Period for Audit Log (Class 1-3)

Audit logs shall be retained onsite at least two (2) months after processing and thereafter archived in accordance with CP § 4.6.2.

4.5.4 Protection of Audit Log (Class 1-3)

Audit logs shall be protected with an electronic audit log system that includes mechanisms to protect the log files from unauthorized viewing, modification, deletion, or other tampering.

4.5.5 Audit Log Backup Procedures (Class 1-3)

Incremental backups of audit logs shall be created daily and full backups weekly.

4.5.6 Audit Collection System (Class 1-3)

No stipulation.

4.5.7 Notification to Event-Causing Subject (Class 1-3)

Where an event is logged by the audit collection system, no notice is required to be given to the individual, organization, device, or application that caused the event.

4.5.8 Vulnerability Assessments (Class 1-3)

Events in the audit process are logged, in part, to monitor system vulnerabilities. Logical security vulnerability assessments (“LSVAs”) shall be performed, reviewed, and revised following an examination of these monitored events. LSVAs shall be based on real-time automated logging data and shall be performed on a daily, monthly, and annual basis in accordance with their definition in the Security and Audit Requirements. An annual LSWA will be an input into an entity’s annual Compliance Audit.

4.6 Records Archival (Class 1-3)

4.6.1 Types of Events Recorded

Records shall be maintained and made available to VeriSign or an entity’s Superior Entity upon request that include:

(i) documentation of the recording entity’s own compliance with the applicable CPS and other obligations under their agreements with their Superior Entities, and

(ii) documentation of actions and information that are material to each Certificate Application and to the creation, issuance, use, revocation, expiration, and renewal of each Certificate it issues. These records shall include all relevant evidence in the recording entity’s possession regarding:

- the identity of the Subscriber named in each Certificate (except for Class 1 Certificates, for which only a record of the Subscriber’s unambiguous name is maintained),
- the identity of persons requesting Certificate revocation (except for Class 1 Certificates, for which only a record of the Subscriber’s unambiguous name is maintained),
- other facts represented in the Certificate,
- time stamps, and
- certain foreseeable material facts related to issuing Certificates including, but not limited to, information relevant to successful completion of a Compliance Audit under CP § 2.7.

Records may be kept in the form of either computer-based messages or paper-based documents, provided their indexing, storage, preservation, and reproduction are accurate and complete.

4.6.2 Retention Period for Archive

Records associated with a Certificate compiled under CP § 4.6.1 shall be retained for at least the time periods set forth below following the date the Certificate expires or is revoked:

- Five (5) years for Class 1 Certificates,
- Ten (10) years for Class 2 Certificates, and
- Thirty (30) years for Class 3 Certificates.

CPSs may contain longer retention periods in order to comply with applicable laws.

4.6.3 Protection of Archive

An entity maintaining an archive of records compiled under CP § 4.6.1 shall protect the archive so that only the entity’s authorized Trusted Persons are able to obtain access to the archive. The archive shall be protected against unauthorized viewing, modification, deletion, or other

tampering by storage within a Trustworthy System. The media holding the archive data and the applications required to process the archive data shall be maintained to ensure that the archive data can be accessed for the time period set forth in CP § 4.6.2.

4.6.4 Archive Backup Procedures

Entities compiling electronic information under CP § 4.6.1 shall incrementally back up system archives of such information on a daily basis and perform full backups on a weekly basis. Copies of paper-based records under CP § 4.6.1 shall be maintained in an off-site disaster recovery facility in accordance with CP § 4.8.

4.6.5 Requirements for Time-Stamping of Records

Certificates, CRLs, and other revocation database entries shall contain time and date information. Such time information need not be cryptographic-based. Note that this use of time-stamping is separate from the VeriSign Digital Notarization Service (*see* CP § 1.1.2.2.2).

4.6.6 Archive Collection System

Archive collection systems for entities within the VTN shall be internal, except for Managed PKI Customers, for which Managed PKI functionality provides external archive collection. Processing Centers shall assist Managed PKI Customers in preserving an audit trail. Such an archive collection system therefore is, to that Managed PKI Customer, external. Otherwise, entities within the VTN shall utilize internal archive collection systems. VeriSign's and Affiliates' CPSs shall require internal audit collection systems for themselves and their Gateway Customers and Managed PKI Customers.

4.6.7 Procedures to Obtain and Verify Archive Information

For information relating to obtaining access to archive information, see CP § 4.6.3.

4.7 Key Changeover (Renewal) (Class 1-3)

A CA Certificate may be renewed if the CA's Superior Entity reconfirms the identity of the CA under CP §§ 3.1.8.2, 3.2.3. Following such reconfirmation, the Superior Entity shall either approve or reject the renewal application.

Following an approval of a renewal request, the Superior Entity itself (in the case of a Processing Center) or through a Processing Center above it in the VTN (in the case of a Service Center) shall conduct a Key Generation Ceremony in order to generate a new key pair for the CA. During such Key Generation Ceremony, the Superior Entity shall sign and issue the CA a new Certificate. Such Key Generation Ceremony shall meet the requirements of the Key Ceremony Reference Guide, the Security and Audit Requirements Guide, and CP § 6.1. New CA Certificates containing the new CA public keys generated during such Key Generation Ceremony shall be made available to Relying Parties in accordance with CP § 6.1.4.

4.8 Compromise and Disaster Recovery (Class 1-3)

Backups of the following CA information shall be kept in off-site storage and made available in the event of a Compromise or disaster: Certificate Application data, audit data (per CP § 4.5), and database records for all Certificates issued. Back-ups of CA private keys shall be generated and maintained in accordance with CP § 6.2.4. Processing Centers shall maintain backups of the foregoing CA information for their own CAs, as well as the CAs of Service Centers, Managed PKI Customers, and ASB Customers within their Subdomains.

4.8.1 Computing Resources, Software, and/or Data Are Corrupted

Following corruption of computing resources, software, and/or data, a report of the event to VeriSign and others, and a response to the event, shall be promptly made by the affected CA or RA in accordance with the incident and Compromise reporting and handling procedures in the applicable CPS and the Security and Audit Requirements Guide (in the case of VeriSign and Affiliates).

4.8.2 Entity Public Key is Revoked

Upon revocation of the Certificate containing the public key of a CA:

- The revocation shall be reported in accordance with CP § 4.4.9 in the VeriSign Repository, and (in the case of non-VeriSign CA's) in the repository of the CA's Superior Entity,
- Commercially reasonable efforts shall be used to provide additional notice of the revocation to VTN Participants, and
- The CA shall perform a key changeover in accordance with CP § 4.7, except following revocation of a CA Certificate in connection with the termination of a CA under CP § 4.9.

4.8.3 Entity Key is Compromised

Upon Compromise of the private key of a VeriSign, Client Service Center, Managed PKI Customer, Gateway Customer CA, or ASB Customer, the CA Certificate of that entity shall be revoked in accordance with CP § 4.4.3.2. Thereafter, reporting of the revocation shall be made in accordance with CP § 4.8.2, and the CA shall cease all use of such private key.

4.8.4 Secure Facility After a Natural or Other Type of Disaster

VTN entities operating secure facilities for CA and RA operations (VeriSign, Affiliates, Managed PKI Customers, and Gateway Customers) shall develop, test, maintain, and, if necessary, implement a disaster recovery plan designed to mitigate the effects of any kind of natural or man-made disaster. Disaster recovery plans shall address the restoration of information systems services and key business functions. Disaster recovery sites shall have the physical security protections specified in the Security and Audit Requirements Guide.

Processing Centers shall have the capability of restoring or recovering operations within twenty-four (24) hours following a disaster with, at a minimum, support for the following functions:

Certificate issuance, Certificate revocation, publication of revocation information, and providing key recovery information for Managed PKI Customers using Managed PKI Key Manager. A Processing Center's disaster recovery database shall be synchronized with the production database within the time limits set forth in the Security and Audit Requirements Guide. A Processing Center's disaster recovery equipment shall have the physical security protections specified in the Security and Audit Requirements Guide, which includes the enforcement of physical security tiers in accordance with CP § 5.1.1.

Service Centers shall have the capability of declaring a disaster on their web sites in their local languages and English, and of directing Subscribers, Relying Parties, and other interested persons to a Processing Center supporting their lifecycle services.

A Service Center or Processing Center disaster recovery plan shall make provisions for the full recovery within one week following disaster occurring at the Service Center's or Processing Center's primary site. Each Service Center and Processing Center shall install and test equipment at its primary site to support CA/RA functions following all but a major disaster that would render the entire facility inoperable. Such equipment shall ensure redundancy and fault tolerance.

4.9 CA Termination (Class 1-3)

The termination of a non-VeriSign CA (Affiliate, Managed PKI Customer, Gateway Customer, or ASB Customer) shall be subject to the contract between the terminating CA and its Superior Entity (or the Superior Entity's Universal Service Center or Reseller). A terminating CA and its Superior Entity shall, in good faith, use commercially reasonable effort to agree on a termination plan that minimizes disruption to Customers, Subscribers, and Relying Parties. The termination plan may cover issues such as:

- Providing notice to parties affected by the termination, such as Subscribers, Relying Parties, and Customers,
- Who bears the cost of such notice, the terminating CA or the Superior Entity,
- The revocation of the Certificate issued to the CA by the Superior Entity,
- The preservation of the CA's archives and records for the time periods required in CP § 4.6,
- The continuation of Subscriber and customer support services,
- The continuation of revocation services, such as the issuance of CRLs or the maintenance of online status checking services,
- The revocation of unexpired unrevoked Certificates of end-user Subscribers and subordinate CAs, if necessary,
- The payment of compensation (if necessary) to Subscribers whose unexpired unrevoked Certificates are revoked under the termination plan or provision, for the issuance of substitute Certificates by a successor CA,
- Disposition of the CA's private key and the hardware token containing such private key, and
- Provisions needed for the transition of the CA's services to a successor CA.

5. Physical, Procedural, and Personnel Security Controls

All entities performing CA and RA functions (VeriSign, Affiliates, Managed PKI Customers, and Gateway Customers) shall draft, implement, and enforce a security policy in accordance with the Security and Audit Requirements Guide (in the case of VeriSign and Affiliates). Each security policy shall discuss physical, procedural, logical, and personnel security controls.

5.1 Physical Controls

5.1.1 Site Location and Construction

All CA and RA operations (by VeriSign, an Affiliate, an Managed PKI Customer, or a Gateway Customer) shall be conducted within a physically protected environment that deters, prevents, and detects unauthorized use of, access to, or disclosure of sensitive information and systems. For VeriSign and Affiliates, this environment shall comply with the requirements in the Security and Audit Requirements Guide.

Such requirements are based in part on the establishment of physical security tiers. A tier is a barrier such as a locked door or closed gate that provides mandatory access control for individuals and requires a positive response (e.g., door unlocks or gate opens) for each individual to proceed to the next area. Each successive tier provides more restricted access and greater physical security against intrusion or unauthorized access. Moreover, each physical security tier encapsulates the next inner tier, such that an inner tier must be fully contained in an outside tier and cannot have a common outside wall with the outside tier, the outermost tier being the outside wall of the building.

5.1.1.1 Gateway Customer Requirements (Class 1)

The facility of a Gateway Customer housing its CA shall have, at a minimum, two physical security tiers, Tier 1 and Tier 2, and Gateway Customers shall perform all cryptographic operations within Tier 2 or higher.

5.1.1.2 Managed PKI Customer Requirements (Class 1-3)

The facility of an Managed PKI Customer that houses its RA functions shall have, at a minimum, two physical security tiers, Tier 1 and Tier 2. All RA validation operations shall be performed in Tier 2 or higher. Managed PKI Customers using Automated Administration, however, shall place the Automated Administration server in Tier 3 or higher space. Moreover, Managed PKI Customers whose Subscribers are using the VeriSign Roaming Service shall have four physical security tiers, Tiers 1 through 4. Enterprise Roaming Servers shall be placed in Tier 4 or higher.

All Managed PKI Customer facilities shall be constructed of materials that will deter, prevent, and detect covert or overt penetration.

5.1.1.3 Service Center Requirements (Class 1-3)

Service Centers shall construct their facilities housing their RA functions with at least four physical security tiers, Tiers 1 through 4. Service Centers shall perform all RA validation

operations within Tier 3 or higher. Service Centers shall place Information Services systems necessary to support CA and/or RA functions in Tier 4 or higher.

Service Centers shall construct their facilities with materials that will deter, prevent, and detect covert or overt penetration. Service Centers' facilities shall meet the minimum building requirements for Service Centers set forth in the Security and Audit Requirements Guide.

5.1.1.4 Processing Center Requirements (Class 1-3)

Processing Centers shall construct their facilities housing their CA functions with at least seven physical security tiers, Tiers 1 through 7. Processing Centers shall perform all RA validation operations within Tier 3 or higher. Processing Centers shall place Information Services systems necessary to support CA functions in Tier 4 or higher. The VeriSign Roaming Server shall be placed in Tier 4 or higher. Processing Centers shall place online and offline CA cryptographic modules in Tier 5 or higher. Processing Centers shall further protect offline CA cryptographic modules by placing them within Tier 7 or higher.

Processing Centers shall construct their facilities with materials that will deter, prevent, and detect covert or overt penetration. Processing Centers' facilities shall meet the minimum building requirements for Processing Centers set forth in the Security and Audit Requirements Guide.

5.1.2 Physical Access

Access to each tier of physical security, constructed in accordance with CP § 5.1.1, shall be controlled so that each tier can be accessed only by authorized personnel in accordance with the Security and Audit Requirements Guide (in the case of VeriSign and Affiliates).

5.1.2.1 Requirements for Gateway Customers (Class 1) and Managed PKI Customers (Class 1-3)

Gateway Customers and Managed PKI Customers shall control access to their CA or RA facilities. The requirements include:

- Minimizing exposure of privileged functions through definition of their function-specific roles or authorization groups,
- Access control enforcement of these roles or groups,
- Use of proximity card identification badges (e.g., Hughes ID),
- Automated logging of access into and out of the facility,
- The use of tamper resistant physical intrusion alarm systems to detect break-ins or unauthorized access to physical security tiers within the facility, and
- Automated notification to outside alarm monitoring agency of a potential security breach when facility-based guards are not present.

Although not required, the use of biometric readers (e.g., hand geometry or iris scan) that provide two-factor authentication is recommended.

5.1.2.2 Service Center Requirements (Class 1-3)

Service Centers shall control access to their CA and/or RA facilities and meet the requirements of CP § 5.1.2.1 and the Service Center requirements in the Security and Audit Requirements Guide.

5.1.2.3 Processing Center Requirements (Class 1-3)

Processing Centers shall control access to their CA and/or RA facilities and meet the requirements of CP § 5.1.2.1 and the Processing Center requirements in the Security and Audit Requirements Guide.

5.1.3 Power and Air Conditioning (Class 1-3)

The secure facilities of VeriSign, Affiliates, Managed PKI Customers, and Gateway Customers shall be equipped with primary and backup power systems to ensure continuous, uninterrupted access to electric power. Also, these secure facilities shall be equipped with primary and backup heating/ventilation/air conditioning systems to control temperature and relative humidity. Such systems shall meet the requirements of the Security and Audit Requirements Guide (in the case of VeriSign and Affiliates).

5.1.4 Water Exposures (Class 1-3)

The secure facilities of VeriSign, Affiliates, Managed PKI Customers, and Gateway Customers shall be constructed and equipped, and procedures shall be implemented, to prevent floods or other damaging exposure to water in accordance with the Security and Audit Requirements Guide (in the case of VeriSign and Affiliates).

5.1.5 Fire Prevention and Protection (Class 1-3)

The secure facilities of VeriSign, Affiliates, Managed PKI Customers, and Gateway Customers shall be constructed and equipped, and procedures shall be implemented, to prevent and extinguish fires or other damaging exposure to flame or smoke in accordance with the Security and Audit Requirements Guide (in the case of VeriSign and Affiliates). These measures shall meet all local applicable safety regulations.

5.1.6 Media Storage (Class 1-3)

VeriSign, Affiliates, Managed PKI Customers, and Gateway Customers shall protect the magnetic media holding back ups of critical system data or any other sensitive information from water, fire, or other environmental hazards, and shall use protective measures to deter, detect, and prevent the unauthorized use of, access to, or disclosure of such media in accordance with the Security and Audit Requirements Guide (in the case of VeriSign and Affiliates).

5.1.7 Waste Disposal (Class 1-3)

VeriSign, Affiliates, Managed PKI Customers, and Gateway Customers shall implement procedures for the disposal of waste (paper, media, or any other waste) to prevent the

unauthorized use of, access to, or disclosure of waste containing Confidential/Private Information within the meaning of CP § 2.8.1 in accordance with the Security and Audit Requirements Guide (in the case of VeriSign and Affiliates).

5.1.8 Off-Site Backup (Class 1-3)

VeriSign, Affiliates, Managed PKI Customers, and Gateway Customers shall maintain back ups of critical system data or any other sensitive information, including audit data, in a secure off-site facility in accordance with the Security and Audit Requirements Guide (in the case of VeriSign and Affiliates).

5.2 Procedural Controls

5.2.1 Trusted Roles

Employees, contractors, and consultants that are designated to manage infrastructural trustworthiness shall be considered to be “Trusted Persons” serving in a “Trusted Position.” Persons seeking to become Trusted Persons by obtaining a Trusted Position shall meet the screening requirements of CP § 5.3.

5.2.1.1 Gateway Customer (Class 1) and Processing Center (Class 1-3) Trusted Roles

Processing Centers and Gateway Customers shall consider the categories of their personnel identified in this Section as Trusted Persons having a Trusted Position. Trusted Persons include all employees, contractors, and consultants that have access to or control authentication or cryptographic operations that may materially affect:

- the validation of information in Certificate Applications;
- the acceptance, rejection, or other processing of Certificate Applications, revocation requests, or renewal requests, or enrollment information;
- the issuance, or revocation of Certificates, including (in the case of Processing Centers) personnel having access to restricted portions of its repository;
- or the handling of Subscriber information or requests.

Trusted Persons also include any other persons identified as such in the Security and Audit Requirements Guide. Trusted Persons include, but are not limited to, customer service personnel, system administration personnel, designated engineering personnel, and executives that are designated to manage infrastructural trustworthiness.

5.2.1.2 Service Center and Managed PKI Customer (Class 1-3) Trusted Roles

Service Centers and Managed PKI Customers shall consider the categories of their personnel identified in this Section as Trusted Persons having a Trusted Position. Trusted Persons include all employees, contractors, and consultants that have access to or control operations that may materially affect:

- the validation of information in Certificate Applications;
- the acceptance, rejection, or other processing of Certificate Applications, revocation requests, or renewal requests, or enrollment information;
- the handling of requests for the revocation of Certificates; or

- the handling of Subscriber information or requests.

Trusted Persons also include any other persons identified as such in the Security and Audit Requirements Guide (in the case of Service Centers). Trusted Persons include, but are not limited to, customer service personnel, system administration personnel, designated engineering personnel, and executives that are designated to manage infrastructural trustworthiness.

5.2.1.3 ASB Customer (Class 2-3) Trusted Roles

ASB Customers shall consider their CA Administrators, which authenticate revocation requests from their Subscribers and communicate such requests to their ASB Customers, to be Trusted Persons having a Trusted Position.

5.2.2 Number of Persons Required Per Task (Class 1-3)

VeriSign, Affiliates, Managed PKI Customers, and Gateway Customers shall establish, maintain, and enforce rigorous control procedures to ensure the segregation of duties based on job responsibility and to ensure that multiple Trusted Persons are required to perform sensitive tasks in accordance with the Security and Audit Requirements Guide (in the case of VeriSign and Affiliates).

5.2.3 Identification and Authentication for Each Role (Class 1-3)

VeriSign, Affiliates, Managed PKI Customers, and Gateway Customers shall confirm the identity and authorization of all personnel seeking to become Trusted Persons in accordance with the Security and Audit Requirements Guide (in the case of VeriSign and Affiliates) before such personnel are:

- issued with their access devices and granted access to the required facilities;
- given electronic credentials to access and perform specific functions on Information Systems and CA or RA systems.

ASB Customers shall confirm the identity and authorization of personnel seeking to become CA Administrators.

Authentication of identity shall include the personal (physical) presence of such personnel before Trusted Persons performing HR or security functions within an entity and a check of well-recognized forms of identification, such as passports and driver's licenses. (This authentication of ASB Customers' CA Administrators, however, shall be performed by members of the ASB Customer's HR or security groups, which need not be Trusted Persons themselves.) Identity shall be further confirmed through background checking procedures in CP § 5.3.1.

5.3 Personnel Controls

5.3.1 Background, Qualifications, Experience, and Clearance Requirements (Class 1-3)

VeriSign, Affiliates, and Customers shall require that personnel seeking to become Trusted Persons present proof of the requisite background, qualifications, and experience needed to perform their prospective job responsibilities competently and satisfactorily, as well as proof of

any government clearances, if any, necessary to perform certification services under government contracts.

5.3.2 Background Check Procedures

VeriSign, Affiliates, and Customers shall conduct background check procedures for personnel seeking to become Trusted Persons in accordance with the Security and Audit Requirements Guide (in the case of VeriSign and Affiliates). Background checks shall be repeated for personnel holding Trusted Positions every three (3) years in the case of background checks performed by private companies or every five (5) years in the case of background checks performed by governmental entities. These procedures shall be subject to any limitations on background checks imposed by local law. To the extent one of the requirements imposed by this section cannot be met due to a prohibition or limitation in local law, the investigating entity shall utilize a substitute investigative technique permitted by law that provides substantially similar information, including but not limited to obtaining a background check performed by the applicable governmental agency.

The factors revealed in a background check that may be considered grounds for rejecting candidates for Trusted Positions or for taking action against an existing Trusted Person are discussed in the Security and Audit Requirements Guide, generally include (but are not limited to) the following:

- Misrepresentations made by the candidate or Trusted Person,
- Highly unfavorable or unreliable professional references,
- Certain criminal convictions, and
- Indications of a lack of financial responsibility.

Reports containing such information shall be evaluated by human resources and security personnel, and such personnel shall take actions, in accordance with the Security and Audit Requirements Guide, that are reasonable in light of the type, magnitude, and frequency of the behavior uncovered by the background check. Such actions may include measures up to and including the cancellation of offers of employment made to candidates for Trusted Positions or the termination of existing Trusted Persons. The use of information revealed in a background check to take such actions shall be subject to applicable law.

5.3.2.1 Background Check Procedures for Gateway Customers (Class 1), ASB Customers (Class 2-3), and Managed PKI Customers (Class 1-3)

Gateway Customers, ASB Customers, and Managed PKI Customers shall perform a background investigation of persons seeking to become a Trusted Person that includes:

- a confirmation of previous employment,
- a check of professional reference,
- a confirmation of the highest or most relevant educational degree obtained,
- a search of criminal records (local, state or provincial, and national), and
- a check of credit/financial records.

5.3.2.2 Background Check Procedures for Service Centers and Processing Centers (Class 1-3)

Service Centers and Processing Centers shall perform a background investigation of persons seeking to become a Trusted Person that includes:

- the matters included in an investigation under CP §§ 5.3.2.1,
- a search of driver's license records, and
- a search of government social insurance records (analogous to Social Security Administration records in the United States or comparable system outside the United States).

5.3.3 Training Requirements (Class 1-3)

VeriSign, Affiliates, and Customers shall provide their personnel with the requisite training prior to being hired, and shall provide the requisite on-the-job training, needed for their personnel to perform their job responsibilities relating to CA or RA operations competently and satisfactorily. They shall also periodically review their training programs, and their training shall address the elements relevant to functions performed by their personnel. Affiliate customer service personnel shall meet VeriSign training requirements, as a condition of the Affiliate beginning operations.

Training programs must address the elements relevant to the particular environment of the person being trained, including:

- Security principles and mechanisms of the VTN and the person's environment,
- Hardware and software versions in use,
- All duties the person is expected to perform,
- Incident and Compromise reporting and handling, and
- Disaster recovery and business continuity procedures.

5.3.4 Retraining Frequency and Requirements (Class 1-3)

VeriSign, Affiliates, and Customers shall provide refresher training and updates to their personnel to the extent and frequency required to ensure that such personnel maintain the required level of proficiency to perform their job responsibilities competently and satisfactorily.

5.3.5 Job Rotation Frequency and Sequence (Class 1-3)

No stipulation.

5.3.6 Sanctions for Unauthorized Actions (Class 1-3)

VeriSign, Affiliates, and Customers shall establish, maintain, and enforce employment policies for the discipline of personnel following unauthorized actions. Disciplinary actions may include measures up to and including termination and shall be commensurate with the frequency and severity of the unauthorized actions.

5.3.7 Contracting Personnel Requirements (Class 1-3)

VeriSign, Affiliates, and Customers shall permit independent contractors or consultants to become Trusted Persons only to the extent necessary to accommodate clearly-defined outsourcing relationships and only under the following conditions:

- (1) the entity using the independent contractors or consultants as Trusted Persons does not have suitable employees available to fill the roles of Trusted Persons, and
- (2) the contractors or consultants are trusted by the entity to the same extent as if they were employees.

Otherwise, independent contractors and consultants shall have access to VeriSign's, an Affiliate's, or a Customer's secure facility only to the extent they are escorted and directly supervised by Trusted Persons.

5.3.8 Documentation Supplied to Personnel (Class 1-3)

VeriSign, Affiliates, and Customers shall give their personnel (including Trusted Persons) the requisite training and other documentation needed to perform their job responsibilities competently and satisfactorily.

6. Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation (Class 1-3)

Key pair generation shall be performed in accordance with this CP § 6.1, using Trustworthy Systems and processes that provide the required cryptographic strength of the generated keys and prevent the loss, disclosure, modification, or unauthorized use of private keys. This requirement applies to end-user Subscribers, Managed PKI Customers using Managed PKI Key Manager, CAs pregenerating key pairs on end-user Subscriber hardware tokens, Processing Centers, and Gateway Customers. Processing Centers generate the CA key pairs of the Client Service Centers, Managed PKI Customers, and ASB Customers in their Subdomains.

CA keys shall be generated in a Key Generation Ceremony. All Key Generation Ceremonies shall conform to the requirements of the Key Ceremony Reference Guide, the CA Key Management Tool User's Guide, and the Security and Audit Requirements Guide.

6.1.2 Private Key Delivery to Entity (Class 1-3)

End-user Subscribers' private keys are generally generated by the end-user Subscribers themselves, and therefore private key delivery to a Subscriber is unnecessary. Private keys shall be delivered to end-user Subscribers only when:

- Their Certificate Applications are approved by a Managed PKI Customer using Managed PKI Key Manager,
- They are Roaming Subscribers, whose private keys are sent to client terminals that they use and decrypted at the client terminals for use in a single session as described in CP § 1.1.2.3.3, or

- Their key pairs are pre-generated on hardware tokens, which are distributed to Certificate Applicants in connection with the enrollment process.

Managed PKI Customers using Managed PKI Key Manager (or an equivalent service approved by VeriSign) shall use the Managed PKI Key Manager Software (or equivalent software approved by VeriSign) and Trustworthy Systems to deliver private keys to Subscribers and shall secure such delivery through the use of a PKCS#12 package or any other comparably equivalent means (e.g., encryption) in order to prevent the loss, disclosure, modification, or unauthorized use of such private keys. Where key pairs are pre-generated on hardware tokens, the entities distributing such tokens shall take commercially reasonable efforts to provide physical security of the tokens to prevent the loss, disclosure, modification, or unauthorized use of the private keys on them.

6.1.3 Public Key Delivery to Certificate Issuer (Class 1-3)

When a public key is transferred to the Gateway Customer or Processing Center to be certified, it shall be delivered through a mechanism ensuring that the public key has not been altered during transit and that the Certificate Applicant possesses the private key corresponding to the transferred public key. The acceptable mechanism within the VTN for public key delivery is a PKCS#10 Certificate signing request package or an equivalent method ensuring that:

1. The public key has not been altered during transit; and
2. The Certificate Applicant possesses the private key corresponding to the transferred public key.

Processing Centers performing Key Generation Ceremonies on behalf of themselves, the Managed PKI Customers, the Service Centers, and ASB Customers within their respective Subdomains shall transfer the public key from the cryptographic module where it was created to the cryptographic module of the superior CA (same cryptographic module if a PCA) by wrapping it in a PKCS#10 Certificate signing request.

6.1.4 CA Public Key Delivery to Users (Class 1-3)

VeriSign and Affiliates shall make the public keys of their CAs and the CAs of the Managed PKI Customers, Gateway Customers, and ASB Customers publicly available to Relying Parties via CA Certificates in a secure fashion. The public keys of the PCAs are included in root Certificates that are already embedded within many popular software applications, making special root distribution mechanisms unnecessary. Also, in many instances, a Relying Party using the S/MIME protocol will automatically receive, in addition to the Subscriber's Certificate, the Certificates (and therefore the public keys) of all CAs subordinate to the relevant PCA.

6.1.5 Key Sizes (Class 1-3)

Key pairs shall be of sufficient length to prevent others from determining the key pair's private key using cryptanalysis during the period of expected utilization of such key pairs. The current VTN Standard for minimum key sizes is the use of key pairs equivalent in strength to 1024 bit RSA for PCAs, CAs, and Class 3 end-user Subscribers and key pairs equivalent in strength to 512 bit RSA for Class 1 and 2 end-user Subscribers.

6.1.6 Public Key Parameters Generation (Class 1-3)

VTN Participants using the Digital Signature Standard shall generate the required Key Parameters in accordance with FIPS 186-2 or a PMA-approved equivalent standard.

6.1.7 Parameter Quality Checking (Class 1-3)

When VTN Participants use the Digital Signature Standard, the quality of the generated Key Parameters shall be verified in accordance with FIPS 186-2 or a PMA-approved equivalent standard.

6.1.8 Hardware/Software Key Generation (Class 1-3)

Processing Centers shall generate Class 2 and 3 CA key pairs (for themselves, Client Service Center, Managed PKI Customers, or ASB Customers), and the random numbers for such key pairs, in hardware. VeriSign recommends that Class 1 CA (Processing Center or Gateway Customer CA), Automated Administration (RA), Administrator, and end-user Subscriber key pairs, and the random numbers for such key pairs, be generated in hardware, although such key pairs may be generated in hardware or software.

6.1.9 Key Usage Purposes (As per X.509 v3 Key Usage Field) (Class 1-3)

For X.509 Version 3 Certificates, Processing Centers and Gateway Customers generally populate the KeyUsage extension of Certificates they issue in accordance with RFC 3280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, April 2002. The KeyUsage extension in X.509 Version 3 VTN Certificates shall be configured so as to set and clear bits and the criticality field in accordance with Table 8 below, although setting the nonrepudiation bit for dual key pair signature Certificates through Managed PKI Key Manager is permissible.

		<i>CAs</i>	<i>Class 1 and Class 2 End-User Subscribers</i>	<i>Automated Administration tokens and Class 2-3 End-User Subscribers</i>	<i>Dual Key Pair Signature (Managed PKI Key Manager)</i>	<i>Dual Key Pair Encipherment (Managed PKI Key Manager)</i>
Criticality		FALSE	FALSE	FALSE	FALSE	FALSE
0	digitalSignature	Clear	Set	Set	Set	Clear
1	nonRepudiation	Clear	Clear	Clear	Clear	Clear
2	keyEncipherment	Clear	Set	Set	Clear	Set
3	dataEncipherment	Clear	Clear	Clear	Clear	Clear
4	keyAgreement	Clear	Clear	Clear	Clear	Clear
5	keyCertSign	Set	Clear	Clear	Clear	Clear
6	CRLSign	Set	Clear	Clear	Clear	Clear
7	encipherOnly	Clear	Clear	Clear	Clear	Clear
8	decipherOnly	Clear	Clear	Clear	Clear	Clear

Table 8 – Settings for KeyUsage Extension

WTLS Certificates and certain CA Certificates are not X.509 Version 3 Certificates and thus do not contain a KeyUsage extension.

Note that although the nonRepudiation bit is not set in the KeyUsage extensions of Certificates issued to Automated Administration tokens, Class 2-3 end-user Subscribers, and the signature Certificate for Subscribers receiving Certificates through Managed PKI Key Manager, the VTN nonetheless supports nonrepudiation services for these Certificates. The nonRepudiation bit is not required to be set in these Certificates because the PKI industry has not reached a consensus as to what the nonRepudiation bit means. Until such a consensus emerges, the nonRepudiation bit will not be meaningful for potential Relying Parties. Moreover, the most commonly used applications do not recognize the nonRepudiation bit. Therefore, setting the bit will not help Relying Parties make a trust decision. Consequently, this CP requires that the nonRepudiation bit be cleared, although it may be set in the case of dual key pair signature Certificates issued through Managed PKI Key Manager.

6.2 Private Key Protection

Private keys shall be protected using a Trustworthy System and private key holders shall take necessary precautions to prevent the loss, disclosure, modification, or unauthorized use of such Private Keys in accordance with this CP § 6.2, the Security and Audit Requirements Guide (in the case of VeriSign and Affiliates). This requirement applies to end-user Subscribers, Managed PKI Customers using Managed PKI Key Manager, Gateway Customers, and Processing Centers, which protect their own private keys and those of the Client Service Centers, Managed PKI Customers, and ASB Customers within their respective Subdomains. End-user Subscribers have the option of protecting their private keys in a smart card or other hardware token. The private keys of Roaming Subscribers, however, reside on an Enterprise Roaming Server in an encrypted form and the symmetric keys to encrypt or decrypt the private key are split between, and reside on, the VeriSign Roaming Server and the Enterprise Roaming Server. VeriSign and Managed PKI Customers shall protect private key segments on these servers using a Trustworthy System.

6.2.1 Standards for Cryptographic Modules (Class 1-3)

Processing Centers shall perform all CA cryptographic operations with their own private keys and the private keys of the Client Service Centers, Managed PKI Customers, and ASB Customers within their Subdomains, on cryptographic modules rated at a minimum of FIPS 140-1 level 2. Service Centers shall perform all RA cryptographic operations on a cryptographic module rated at FIPS 140-1 level 2. VeriSign recommends that Managed PKI Customers perform all Automated Administration RA cryptographic operations on a cryptographic module rated at FIPS 140-1 level 2 and that Gateway Class 1 Customers perform all CA cryptographic operations on a cryptographic module rated at FIPS 140-1 level 1. The requirements for ratings in this section are subject to any applicable local requirements for higher ratings.

6.2.2 Private Key (m out of n) Multi-Person Control (Class 1-3)

Multi-person control shall be enforced to protect the activation data needed to activate CA private keys held by Processing Centers in accordance with the Key Ceremony Reference Guide and Security and Audit Requirements Guide. Processing Centers shall use “Secret Sharing” to split the private key or activation data needed to operate the private key into separate parts called “Secret Shares” held by individuals called “Shareholders.” Some threshold number of Secret Shares (m) out of the total number of Secret Shares (n) shall be required to operate the private key.

Processing Centers shall utilize Secret Sharing to protect the activation data needed to activate their own private keys, and those of the Client Service Centers, Managed PKI Customers, and ASB Customers within their respective Subdomains, in accordance with the Key Ceremony Reference Guide and Security and Audit Requirements Guide. Processing Centers shall also use Secret Sharing to protect the activation data needed to activate private keys located at their respective disaster recovery sites. Processing Centers shall implement Secret Sharing.

The threshold number of shares needed to sign a CA certificate is 3. It should be noted that the number of shares distributed for disaster recovery tokens may be less than the number distributed for operational tokens, while the threshold number of required shares remains the same. Secret Shares are protected in accordance with CP § 6.4.2.

6.2.3 Private Key Escrow (Class 1-3)

Managed PKI Customers using the Managed PKI Key Management service (or an equivalent service approved by VeriSign) are permitted to escrow end-user Subscribers’ private key as described in CP §1.1.2.3.2.. Escrowed private keys shall be stored in encrypted form using the Managed PKI Key Manager software. Except for Managed PKI Customers using the Managed PKI Key Manager Service (or an equivalent service approved by VeriSign), the private keys of CAs or end-user Subscribers shall not be escrowed.

End-user Subscriber private keys shall only be recovered under the circumstances permitted within the Managed PKI Key Management Service Administrator’s Guide, under which:

- Managed PKI Customers using Managed PKI Key Manager shall confirm the identity of any person purporting to be the Subscriber to ensure that a purported Subscriber request for the Subscriber’s private key is, in fact, from the Subscriber and not an imposter,
- Such Managed PKI Customers shall recover a Subscriber’s private key without the Subscriber’s request only for their legitimate and lawful purposes, such as to comply with judicial or administrative process or a search warrant, and not for any illegal, fraudulent, or other wrongful purpose, and
- Such Managed PKI Customers shall have personnel controls in place to prevent Key Management Service Administrators and other persons from obtaining unauthorized access to private keys.

6.2.4 Private Key Backup (Class 1-3)

Processing Centers and Gateway Customers shall back up their own private keys so as to be able to recover from disasters and equipment malfunction in accordance with the Key Ceremony Reference Guide and Security and Audit Requirements Guide. Processing Centers shall also back up the private keys of Client Service Centers, Managed PKI Customers, and ASB Customers within their Subdomains in accordance with these documents. Back-ups shall be made by copying such private keys and entering them onto back-up cryptographic modules in accordance with CP § 6.2.6.

Private keys that are backed up are to be protected from unauthorized modification or disclosure through physical or cryptographic means. Back ups shall be protected with a level of physical and cryptographic protection equal to or exceeding that for cryptographic modules within the Processing Center's or Gateway Customer's CA site, such as at a disaster recovery site or at another secure facility off-site, such as a bank safe.

The backup of end-user Subscriber private keys subject to the Managed PKI Key Manager service, is governed by CP § 6.2.3. VeriSign recommends that Managed PKI Customers having Automated Administration tokens and Class 3 end-user Subscribers who are not subject to the Managed PKI Key Manager service back up their private keys and protect them from unauthorized modification or disclosure by physical or cryptographic means. The database of encrypted private keys stored on an Enterprise Roaming Server and the databases of segments of symmetric keys (used to encrypt and decrypt these private keys) stored on the VeriSign Roaming Server and Enterprise Roaming Servers shall be backed up for disaster recovery and business continuity purposes.

6.2.5 Private Key Archival (Class 1-3)

No stipulation.

6.2.6 Private Key Entry into Cryptographic Module (Class 1-3)

The mechanisms of entry of a private key into a cryptographic module shall prevent loss, theft, modification, unauthorized disclosure, or unauthorized use of such private key. CA or RA private keys held on hardware cryptographic modules shall be stored in encrypted form.

Processing Centers generating CA or RA private keys on one hardware cryptographic module and transferring them into another shall securely transfer such private keys into the second cryptographic module to the extent necessary to prevent loss, theft, modification, unauthorized disclosure, or unauthorized use of such private keys. Such transfers shall be limited to making backup copies of the private keys on tokens in accordance with the Security and Audit Requirements and the Key Ceremony Reference Guide. Private keys shall be encrypted during such transfer.

VTN Participants pregenerating private keys and transferring them into a hardware token, for example transferring generated end-user Subscriber private keys into a smart card, shall securely

transfer such private keys into the token to the extent necessary to prevent loss, theft, modification, unauthorized disclosure, or unauthorized use of such private keys.

6.2.7 Method of Activating Private Key

All VTN Participants shall protect the activation data for their private keys against loss, theft, modification, unauthorized disclosure, or unauthorized use.

6.2.7.1 End-User Subscriber Private Keys

This section states the VTN Standards for protecting activation data for end-user Subscribers' private keys, although Subscribers have the option of using enhanced private key protection mechanisms available today including the use of smart cards, biometric access devices, and other hardware tokens to store private keys.

6.2.7.1.1 Class 1 Certificates

The VTN Standard for Class 1 private key protection is for Subscribers to take commercially reasonable measures for the physical protection of the Subscriber's workstation to prevent use of the workstation and its associated private key without the Subscriber's authorization. In addition, VeriSign recommends that Subscribers use a password in accordance with CP § 6.4.1.1 or security of equivalent strength to authenticate the Subscriber before the activation of the private key, which includes, for instance, a password to operate the private key, a Windows logon or screen saver password, or a network logon password.

6.2.7.1.2 Class 2 Certificates

The VTN Standard for Class 2 Private Key protection is for Subscribers to:

- Use a password in accordance with CP § 6.4.1.1 or security of equivalent strength to authenticate the Subscriber before the activation of the private key, which includes, for instance, a password to operate the private key, a Windows logon or screen saver password, a network logon password, or a password in conjunction with the VeriSign Roaming Service; and
- Take commercially reasonable measures for the physical protection of the Subscriber's workstation to prevent use of the workstation and its associated private key without the Subscriber's authorization.

When deactivated, private keys shall be kept in encrypted form only.

6.2.7.1.3 Class 3 Certificates Other Than Administrator Certificates

The VTN Standard for Class 3 private key protection (other than Administrators) is for Subscribers to:

- Use a smart card, biometric access device, password in conjunction with the VeriSign Roaming Service, or security of equivalent strength to authenticate the Subscriber before the activation of the private key; and

- Take commercially reasonable measures for the physical protection of the Subscriber's workstation to prevent use of the workstation and its associated private key without the Subscriber's authorization.

Use of a password along with a smart card or biometric access device in accordance with CP § 6.4.1.1 is recommended. When deactivated, private keys shall be kept in encrypted form only.

6.2.7.2 Administrators' Private Keys (Class 3)

6.2.7.2.1 Administrators

The VTN Standard for Administrators' private key protection requires them to:

- Use a smart card, biometric access device, password in accordance with CP § 6.4.1.2, or security of equivalent strength to authenticate the Administrator before the activation of the private key, which includes, for instance, a password to operate the private key, a Windows logon or screen saver password, or a network logon password; and
- Take commercially reasonable measures for the physical protection of the Administrator's workstation to prevent use of the workstation and its associated private key without the Administrator's authorization.

VeriSign recommends that Administrators use a smart card, biometric access device, or security of equivalent strength along possibly with the use of a password in accordance with CP § 6.4.1.2 to authenticate the Administrator before the activation of the private key.

When deactivated, private keys shall be kept in encrypted form only.

6.2.7.2.2 Managed PKI Administrators using a Cryptographic Module (with Automated Administration or with Managed PKI Key Manager Service)

The VTN Standard for private key protection for Administrators using such a cryptographic module requires them to:

- Use the cryptographic module along with a password in accordance with CP § 6.4.1.2 to authenticate the Administrator before the activation of the private key; and
- Take commercially reasonable measures for the physical protection of the workstation housing the cryptographic module reader to prevent use of the workstation and the private key associated with the cryptographic module without the Administrator's authorization.

6.2.7.3 Gateway Customers' Private Keys (Class 1)

The VTN Standard for Gateway Customers private key protection requires them to:

- Use a password (or security of equivalent strength) in accordance with CP § 6.4.1.3 to authenticate the Gateway Customer before the activation of the private key, which is associated with an account with administrator privileges on the Gateway server; and
- Take commercially reasonable measures for the physical protection of the Gateway server to prevent use of the server and the private key associated with the server without the Gateway Customer's authorization.

Once the private key is activated, the private key can be active for an indefinite period until deactivated when the Gateway CA system goes offline.

6.2.7.4 Private Keys Held by Processing Centers (Class 1-3)

This section applies to a Processing Center's own CAs and of the CAs of the Client Service Centers, Managed PKI Customers, and ASB Customers within its Subdomain. An online CA's private key shall be activated by a threshold number of Shareholders, as defined in CP § 6.2.2, supplying their activation data (stored on secure media). Once the private key is activated, the private key may be active for an indefinite period until it is deactivated when the CA goes offline. Similarly, a threshold number of Shareholders shall be required to supply their activation data in order to activate an offline CA's private key. Once the private key is activated, it shall be active only for one time.

6.2.8 Method of Deactivating Private Key

6.2.8.1 End-User Subscribers

6.2.8.1.1 Class 1 Certificates

No stipulation.

6.2.8.1.2 Class 2 Certificates

No stipulation.

6.2.8.1.3 Class 3 Certificates

End-user Subscribers have an obligation to protect their private keys under CP § 6.2.7.1. Such obligations extend to protection of the private key after a private key operation has taken place.

6.2.8.2 Gateway Customers (Class 1)

No stipulation

6.2.8.3 Processing Centers (Class 1-3)

This section applies to a Processing Center's own CAs and of the CAs of the Client Service Centers, Managed PKI Customers, and ASB Customers within its Subdomain. When an online CA is taken offline, the Processing Center's personnel shall remove the token containing such CA's private key from the reader in order to deactivate it. With respect to the private keys of offline CAs, after the completion of a Key Generation Ceremony (*see* CP § 6.1.1) in which such private keys are used for private key operations, the Processing Center's personnel shall remove the token containing such CAs' private keys from the reader in order to deactivate them. Once removed from the reader, tokens shall be protected in accordance to the Security and Audit Requirements Guide.

6.2.9 Method of Destroying Private Key

Private keys shall be destroyed in a way that prevents their loss, theft, modification, unauthorized disclosure, or unauthorized use.

6.2.9.1 Gateway Customers (Class 1)

Gateway Customers shall decommission their private keys upon termination of CA operations to prevent loss, theft, modification, unauthorized disclosure, or unauthorized use.

6.2.9.2 Processing Centers (Class 1-3)

Upon termination of the operations of a Processing Center's CA, or that of a Client Service Center, Managed PKI Customer, or ASB Customer within its Subdomain, Processing Center personnel shall decommission the CA's private key by deleting it using functionality of the token containing such CA's private key so as to prevent its recovery following deletion, or the loss, theft, modification, unauthorized disclosure, or unauthorized use of such private key, while not adversely affecting the private keys of other CAs contained on the token. This process shall be witnessed in accordance with the Security and Audit Requirements Guide and the Key Ceremony Reference Guide.

6.3 Other Aspects of Key Pair Management (Class 1-3)

6.3.1 Public Key Archival

Processing Centers shall archive their own public keys, as well as the public keys of all of the Client Service Centers, Managed PKI Customers, and ASB Customers within their Subdomains, in accordance with CP § 4.6. Gateway Customers shall archive their public keys in accordance with CP § 4.6.

6.3.2 Usage Periods for the Public and Private Keys

The Operational Period for Certificates shall be set to the time limits set forth in Table 9 below. As necessary to ensure the security of the VTN, VeriSign shall commission new PCAs. The new PCAs' Certificates' Operational Periods shall be defined based in part on forecasts of new industry leading browser version developments.

The usage period for end-user Subscriber key pairs is the same as the Operational Period for their Certificates, except that private keys may continue to be used after the Operational Period to decrypt messages sent to the Subscriber during the Operational Period. Note that the Operational Period of a Certificate ends upon its expiration or revocation. A CA, however, shall not issue Certificates if their Operational Periods would extend beyond the usage period of the key pair of the CA. Therefore, the CA key pair usage period is necessarily shorter than the operational period of the CA Certificate. Specifically, the usage period is the Operational Period of the CA Certificate minus the Operational Period of the Certificates that the CA issues. Upon the end of the usage period for a Subscriber or CA key pair, the Subscriber or CA shall thereafter cease all use of the key pair, except to the extent a CA needs to sign revocation information until the end of the Operational Period of the last Certificate it has issued.

Certificate Issued By:	Class 1	Class 2	Class 3
PCA self-signed	Up to 30 years	Up to 30 years	Up to 30 years
PCA to CA	Up to 10 years	Up to 10 years	Up to 10 years
CA to Subordinate CA	Up to 5 years	Up to 5 years	Up to 5 years
CA to End-user Subscriber	Up to 2 years	Normally up to 2 years, but under the conditions described below, up to 5 years	Normally up to 2 years, but under the conditions described below, up to 5 years
CA to end-user organizational automated administration certificate	N/A	N/A	Up to 5 years

Table 9 – Certificate Operational Periods

Except as noted in this section, VTN Participants shall cease all use of their key pairs after their usage periods have expired.

Certificates issued by CAs to end-user Subscribers may have Operational Periods longer than two years, up to five years, if the following requirements are met:

- The Certificates are individual Certificates,
- Subscribers’ key pairs reside on a hardware token, such as a smart card,
- Subscribers are annually required to undergo reauthentication procedures under CP § 3.1.9,
- Subscribers shall annually prove possession of the private key corresponding to the public key within the Certificate,
- If a Subscriber is unable to complete reauthentication procedures under CP § 3.1.9 successfully or is unable to prove possession of such private key when required by the foregoing, the CA shall automatically revoke the Subscriber’s Certificate.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

VTN Participants generating and installing activation data for their private keys shall use methods that protect the activation data to the extent necessary to prevent the loss, theft, modification, unauthorized disclosure, or unauthorized use of such private keys.

6.4.1.1 End-User Subscribers (Class 1-3)

To the extent passwords are used as activation data (*see* CP § 6.2.7.1), Subscribers shall generate passwords that cannot easily be guessed or cracked by dictionary attacks. VeriSign and Affiliates shall provide information to Subscribers in their Subdomain concerning methods to

choose secure passwords. Note that Class 3 end-user Subscribers may not need to generate activation data, for example if they use biometric access devices.

6.4.1.2 Administrators (Class 3)

Activation data use by Administrators shall meet the requirements of CP § 6.4.1.1.

6.4.1.3 Gateway Customers (Class 1)

Gateway Customers shall generate activation data in accordance with CP § 6.2.7.3. Gateway Customers shall use passwords as activation data that cannot easily be guessed or cracked by dictionary attacks.

6.4.1.4 Processing Centers (Class 1-3)

Processing Centers shall generate activation data for their own CAs' private keys, and for the private keys of Client Service Centers, Managed PKI Customers, and ASB Customers within their Subdomains, in accordance with the Secret Sharing requirements of CP § 6.2.2, the Key Ceremony Reference Guide, and the Security and Audit Requirements Guide.

6.4.2 Activation Data Protection

VTN Participants shall protect the activation data for their private keys using methods that protect against the loss, theft, modification, unauthorized disclosure, or unauthorized use of such private keys.

6.4.2.1 End-User Subscribers (Class 1-3) and Gateway Customers (Class 1)

End-user Subscribers and Gateway Customers shall protect the activation data for their private keys, if any, to the extent necessary to prevent the loss, theft, modification, unauthorized disclosure, or unauthorized use of such private keys.

6.4.2.2 Processing Centers (Class 1-3)

Processing Centers shall utilize Secret Sharing in accordance with CP § 6.2.2 and the Security and Audit Requirements Guide. Processing Centers shall provide the procedures and means to enable Shareholders to take the precautions necessary to prevent the loss, theft, modification, unauthorized disclosure, or unauthorized use of the Secret Shares that they possess.

Shareholders shall not:

- Copy, disclose, or make the Secret Share available to a third party, or make any unauthorized use of it whatsoever; or
- disclose his, her, or any other person's status as a Shareholder to any third party.

The Secret Shares and any information disclosed to the Shareholder in connection with his or her duties as a Shareholder shall constitute Confidential/Private Information under CP § 2.8.1.

Also, Processing Centers shall include in their disaster recovery plans provisions for Shareholders making their Secret Shares available at a disaster recovery site after a disaster.

Each Processing Center shall maintain an audit trail of Secret Shares, and Shareholders shall participate in the maintenance of an audit trail.

6.4.3 Other Aspects of Activation Data (Class 1-3)

6.4.3.1 Activation Data Transmission

To the extent activation data for their private keys are transmitted, VTN Participants shall protect the transmission of such activation data for their private keys using methods that protect against the loss, theft, modification, unauthorized disclosure, or unauthorized use of such private keys. For example, Processing Centers shall ensure the transfer of Secret Shares be performed in accordance with CP § 6.4.2. Also, to the extent Windows or network logon user name/password combination is used as activation data for an end-user Subscriber or Gateway Customer, the passwords transferred across a network shall be protected against access by unauthorized users.

6.4.3.2 Activation Data Destruction

Activation data for CA private keys shall be decommissioned using methods that protect against the loss, theft, modification, unauthorized disclosure, or unauthorized use of the private keys protected by such activation data. After the record retention periods in CP § 4.6 expire, Processing Centers shall decommission activation data by overwriting or physical destruction.

6.5 Computer Security Controls

CA and RA functions shall take place on Trustworthy Systems in accordance with the Security and Audit Requirements Guide (in the case of VeriSign and Affiliates).

6.5.1 Specific Computer Security Technical Requirements

6.5.1.1 Controls for Processing Centers (Class 1-3)

Processing Centers shall ensure that the systems maintaining CA software and data files are Trustworthy Systems secure from unauthorized access, which can be demonstrated by compliance with audit criteria applicable under CP § 2.7.4. In addition, Processing Centers shall limit access to production servers to those individuals with a valid business reason for access. General application users shall not have accounts on the production servers.

Processing Centers shall have production networks logically separated from other components. This separation prevents network access except through defined application processes. Processing Centers shall use firewalls to protect the production network from internal and external intrusion and limit the nature and source of network activities that may access production systems. Processing Centers shall require the use of passwords with a minimum character length and a combination of alphanumeric and special characters, and shall require that passwords be changed on a periodic basis and whenever necessary. Direct access to a Processing Center's database maintaining the Processing Center's repository shall be limited to Trusted Persons in the Processing Center's operations group having a valid business reason for such access.

6.5.1.2 Controls for Gateway Customers (Class 1)

Gateway servers shall include the following functionality:

- access control to CA services,
- identification and authentication for launching of CA services,
- object re-use for CA random access memory,
- use of cryptography for session communication and database security,
- archival of CA and end-user Subscriber history and audit data,
- audit of security related events,
- self-test of security related CA services, and
- trusted path for identification of PKI roles and associated identities.

6.5.1.3 Controls for Service Centers and Managed PKI Customers (Class 1-3)

Service Centers and Managed PKI Customers shall ensure that the systems maintaining RA software and data files are Trustworthy Systems secure from unauthorized access, which can be demonstrated by compliance with audit criteria applicable under CP § 2.7.4.

Service Centers and Managed PKI Customers shall logically separate access to these systems and this information from other components. This separation prevents access except through defined processes. Service Centers and Managed PKI Customers shall use firewalls to protect the network from internal and external intrusion and limit the nature and source of activities that may access such systems and information. Service Centers and Managed PKI Customers shall require the use of passwords with a minimum character length and a combination of alphanumeric and special characters, and shall require that passwords be changed on a periodic basis and as necessary. Direct access to the Service Center's or Managed PKI Customer's RA database maintaining Subscriber information shall be limited to Trusted Persons in the Service Center's or Managed PKI Customer's operations group having a valid business reason for such access.

6.5.2 Computer Security Rating (Class 1-3)

Specific security sensitive areas of the CA and RA functionality of VeriSign-supplied software shall meet the assurance requirements EAL 3 (Common Criteria for Information Technology Security Evaluation, v 2.1, Aug. 1999).

6.6 Life Cycle Technical Controls (Class 1-3)

6.6.1 System Development Controls

6.6.1.1 Software Used by Gateway Customers

No stipulation.

6.6.1.2 Software Used by Managed PKI Customers, Service Centers, and Processing Centers

VeriSign provides software for CA and RA functions to Processing Centers, Service Centers, and Managed PKI Customers. Such software, to the extent used to manage Class 2 or 3 Certificates, shall be developed within systems development environments that meet VeriSign's development assurance requirements. VeriSign shall use a design and development process that enforces quality assurance and process correctness.

The software provided by VeriSign to Managed PKI Customers, Service Centers, and Processing Centers, when first loaded, shall provide a method for the entity to verify that the software on the system:

- originated from VeriSign,
- has not been modified prior to installation, and
- is the version intended for use.

6.6.2 Security Management Controls

6.6.2.1 Software Used by Gateway Class 1 Customers

No stipulation.

6.6.2.2 Software Used by Managed PKI Customers, Service Centers, and Processing Centers

Software for CA and RA functions designed to manage Class 2 or 3 Certificates shall be subject to checks to verify its integrity. VeriSign shall provide a hash of all software packages or software updates it provides to Managed PKI Customers, Service Centers, and Processing Centers. This hash can be used to verify the integrity of such software manually. Processing Centers shall also have mechanisms and/or policies in place to control and monitor the configuration of their CA systems. Upon installation, and at least once a day, Processing Centers shall validate the integrity of the CA system.

6.6.3 Life Cycle Security Ratings

No stipulation.

6.7 Network Security Controls (Class 1-3)

VeriSign, Affiliates, Managed PKI Customers, and Gateway Customers shall perform CA and RA functions using networks secured in accordance with the Security and Audit Requirements Guide (in the case of VeriSign and Affiliates) to prevent unauthorized access, tampering, and denial-of-service attacks. VeriSign, Affiliates, and Customers shall protect their communications of sensitive information using point-to-point encryption for confidentiality and digital signatures for non-repudiation and authentication.

6.8 Cryptographic Module Engineering Controls (Class 1-3)

See CP § 6.2.1.

7. Certificate and CRL Profile (Class 1-3)

7.1 Certificate Profile

VTN Certificates shall have the profile and contain the fields specified in this CP § 7.1. Except for WTLS Certificates, VTN Certificates shall conform to (a) ITU-T Recommendation X.509 (1997): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, June 1997 and (b) RFC 3280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, April 2002 (“RFC 3280”).

At a minimum, X.509 VTN Certificates shall contain the basic fields and indicated prescribed values or value constraints in Table 10 below:

<i>Field</i>	<i>Value or Value constraint</i>
Serial Number	Unique value per Issuer DN
Signature Algorithm	Object identifier of the algorithm used to sign the certificate (See CP § 7.1.3)
Issuer DN	See CP § 7.1.4
Valid From	Universal Coordinate Time base. Synchronized to Master Clock of U.S. Naval Observatory. Encoded in accordance with RFC 3280.
Valid To	Universal Coordinate Time base. Synchronized to Master Clock of U.S. Naval Observatory. Encoded in accordance with RFC 3280.
Subject DN	See CP § 7.1.4
Subject Public Key	Encoded in accordance with RFC 3280
Signature	Generated and encoded in accordance with RFC 3280

Table 10 – Certificate Profile Basic Fields

WTLS Certificates conformed to the most current version of the Wireless Application Protocol.

Processing Centers and Gateway Customers shall issue Certificates having the profile set forth in this CP § 7.1. In addition, Processing Centers shall issue Certificates having such profile for their own CAs and the CAs of Client Service Centers, Managed PKI Customers, and ASB Customers within their Subdomains.

7.1.1 Version Number(s)

Except for WTLS Certificates, that conformed to the most current version of the Wireless Application Protocol, all VTN Certificates shall be X.509 Version 3 Certificates although certain Root Certificates are permitted to be X.509 Version 1 Certificates to support legacy systems. Processing Centers shall issue X.509 Version 1 or Version 3 CA Certificates. Also, Processing

Centers and Gateway Customers shall issue X.509 Version 3 end-user Subscriber Certificates. Processing Centers shall issue WTLS Certificates.

7.1.2 Certificate Extensions

Processing Centers and Gateway Customers shall populate X.509 Version 3 VTN Certificates with the extensions required by CP §§ 7.1.2.1-7.1.2.8. Private extensions are permissible, but the use of a private extension(s) is not warranted under this CP and the applicable CPS unless specifically included by reference.

7.1.2.1 Key Usage

Processing Centers and Gateway Customers shall populate the KeyUsage extension of X.509 Version 3 CA, Automated Administration, and end-user Subscriber Certificates by setting and clearing the bit(s) and the criticality field in accordance with CP § 6.1.9. The criticality field of this extension is generally set to FALSE.

7.1.2.2 Certificate Policies Extension

Processing Centers and Gateway Customers shall populate the CertificatePolicies extension of X.509 Version 3 CA, Automated Administration, and end-user Subscriber Certificates with the object identifier of this CP in accordance with CP § 7.1.6 and with policy qualifiers set forth in CP § 7.1.8. The criticality field of this extension shall be set to FALSE.

7.1.2.3 Subject Alternative Names

Processing Centers and Gateway Customers shall populate the subjectAltName extension of X.509 Version 3 CA, Automated Administration, and end-user Subscriber Certificates in accordance with RFC 3280. The criticality field of this extension shall be set to FALSE.

7.1.2.4 Basic Constraints

Processing Centers shall populate X.509 Version 3 CA Certificates with a BasicConstraints extension with the CA field set to TRUE. Processing Centers and Gateway Customers shall populate end-user Subscriber Certificates with a BasicConstraints extension, but the extension shall be given a value of an empty sequence. The criticality field of this extension shall be set to TRUE for CA Certificates, but otherwise set to FALSE.

X.509 Version 3 CA Certificates issued to PCAs, Processing Centers, and Client Service Centers shall have a “pathLenConstraint” field of the BasicConstraints extension set to the maximum number of CA certificates that may follow this Certificate in a certification path. CA Certificates issued to the online CAs of Managed PKI Customers and Gateway Customers issuing end-user Subscriber Certificates shall have a “pathLenConstraint” field set to a value of “0” indicating that only an end-user Subscriber Certificate may follow in the certification path.

7.1.2.5 Extended Key Usage

Processing Centers and Gateway Customers, shall populate X.509 Version 3 VTN End-Entity Certificates with an ExtendedKeyUsage extension configured to include the key purpose object identifiers (OID) shown in Table 11 below. Except where specifically described below, this extension is usually not included in end-entity certificates. By default, ExtendedKeyUsage is set as a non-critical extension. VTN CA Certificates do not include the ExtendedKeyUsage extension.

	<i>Class 1-3 Client Certificates, RA Certificates issued to Automated Administration tokens, and Class 3 Organizational ASB Certificates</i>	<i>Object Signing Class 3 Organizational Certificates</i>	<i>Other Class 3 Organizational Certificates (e.g., Secure Server IDs and Global Server IDs)</i>
ServerAuth (1.3.6.1.5.5.7.3.1)	Not Included	Not Included	Included
ClientAuth (1.3.6.1.5.5.7.3.2)	Included	Not Included	Included
CodeSigning (1.3.6.1.5.5.7.3.3)	Not Included	Included	Not Included
EmailProtection (1.3.6.1.5.5.7.3.4)	Included	Not Included	Not Included
TimeStamping (1.3.6.1.5.5.7.3.8)	Not Included	Not Included	Not Included

Table 11 – Types of Key Purposes Included in ExtendedKeyUsage Extension

7.1.2.6 CRL Distribution Points

Processing Centers and Gateway Customers, shall populate X.509 Version 3 VTN Certificates with a cRLDistributionPoints extension containing the URL of the location where a Relying Party can obtain a CRL to check the Certificate’s status. The criticality field of this extension shall be set to FALSE.

7.1.2.7 Authority Key Identifier

Processing Centers and Gateway Customers generally populate X.509 Version 3 VTN Certificates with an authorityKeyIdentifier extension, and the method for generating the keyIdentifier based on the public key of the CA issuing the Certificate shall be calculated in accordance with one of the methods described in RFC 3280. The criticality field of this extension shall be set to FALSE.

7.1.2.8 Subject Key Identifier

If Processing Centers or Gateway Customers populate X.509 Version 3 VTN Certificates with a subjectKeyIdentifier extension, the method for generating the keyIdentifier based on the public key of the Subject of the Certificate shall be calculated in accordance with one of the methods

described in RFC 3280. If present, the criticality field of this extension, if present, shall be set to FALSE.

7.1.3 Algorithm Object Identifiers

Processing Centers and Gateway Customers shall sign VTN Certificates using one of following algorithms.

sha-1WithRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}

md5WithRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 4}

md2WithRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 2}

Certificate signatures produced using these algorithms shall comply with RFC 3279. Use of sha-1WithRSAEncryption shall be given strong preference over md5WithRSAEncryption. Use of md5WithRSAEncryption shall be given very strong preference over md2WithRSAEncryption (which was used to sign certain legacy CA and End-User Subscriber Certificates)

7.1.4 Name Forms

Processing Centers and Gateway Customers shall populate VTN Certificates with the name required under CP § 3.1.1. In addition, Processing Centers and Gateway Customers shall include within end-user Subscriber Certificates an additional Organizational Unit field that contains a notice stating that the terms of use of the Certificate are set forth in a URL, and the URL shall be a pointer to the applicable Relying Party Agreement. Exceptions to the foregoing requirement shall be permitted only when space, formatting, or interoperability limitations within Certificates make such an Organizational Unit impossible to use in conjunction with the application for which the Certificates are intended.

7.1.5 Name Constraints

No stipulation.

7.1.6 Certificate Policy Object Identifier

The object identifier for the Certificate policy corresponding to each Class of Certificate is set forth in CP § 1.2. Processing Centers and Gateway Customers shall populate the CertificatePolicies extension in each X.509 Version 3 VTN Certificate with the object identifier of the Certificate policy corresponding to the Certificate's class set forth in CP § 1.2.

7.1.7 Usage of Policy Constraints Extension

No stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

Processing Centers and Gateway Customers shall populate all X.509 Version 3 VTN Certificates with a policy qualifier within their CertificatePolicies extensions. Specifically, such Certificates shall contain a CPS pointer qualifier populated with a URL pointing to the applicable Relying Party Agreement.

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

No stipulation.

7.2 CRL and OCSP Profile

Processing Centers and Gateway Customers shall issue CRLs that conform to RFC 3280 and OCSP responders that conform with RFC2560.

7.2.1 Version Number(s)

No stipulation.

7.2.2 CRL and CRL Entry Extensions

No stipulation.

8. Specification Administration (Class 1-3)

8.1 Specification Change Procedures

Amendments to this CP shall be made by the VeriSign Trust Network Policy Management Authority. Amendments shall either be in the form of a document containing an amended form of the CP or an update. Amended versions or updates shall be linked to the Practices Updates and Notices section of the VeriSign Repository located at:

<https://www.verisign.com/repository/updates>. Updates supersede any designated or conflicting provisions of the referenced version of the CP. The PMA shall determine whether changes to the CP require a change in the Certificate policy object identifiers of the Certificate policies corresponding to each Class of Certificate.

8.1.1 Items that Can Change Without Notification

VeriSign and the PMA reserve the right to amend the CP without notification for amendments that are not material, including without limitation corrections of typographical errors, changes to URLs, and changes to contact information. The PMA's decision to designate amendments as material or non-material shall be within the PMA's sole discretion.

8.1.2 Items that Can Change with Notification

The PMA shall make material amendments to the CP in accordance with this Section 8.1.2.

8.1.2.1 List of Items

Material amendments are those changes that the PMA, under CP § 8.1.1, considers to be material.

8.1.2.2 Notification Mechanism

The PMA shall send Affiliates notice of material amendments to the CP proposed by the PMA. The notice shall state the text of the proposed amendments and the comment period under Section 8.1.2.3. Proposed amendments to the CP shall also appear in the Practices Updates and Notices section of the VeriSign Repository, which is located at:

<https://www.verisign.com/repository/updates>. Affiliates shall publish or provide a link to the proposed amendments on their own web-based repositories within a reasonable time after receiving notice of such amendments.

The PMA solicits proposed amendments to the CP from other VTN Participants. If the PMA considers such an amendment desirable and proposes to implement the amendment, the PMA shall provide notice of such amendment in accordance with this section.

Notwithstanding anything in the CP to the contrary, if the PMA believes that material amendments to the CP are necessary immediately to stop or prevent a breach of the security of the VTN or any portion of it, VeriSign and the PMA shall be entitled to make such amendments by publication in the VeriSign Repository. Such amendments will be effective immediately upon publication. Within a reasonable time after publication, VeriSign shall provide notice to Affiliates of such amendments.

8.1.2.3 Comment Period

Except as noted under CP § 8.1.2.2, the comment period for any material amendments to the CP shall be fifteen (15) days, starting on the date on which the amendments are posted on the VeriSign Repository. Any VTN Participant shall be entitled to file comments with the PMA up until the end of the comment period.

8.1.2.4 Mechanism to Handle Comments

The PMA shall consider any comments on the proposed amendments. The PMA shall either (a) allow the proposed amendments to become effective without amendment, (b) amend the proposed amendments and republish them as a new amendment under CP § 8.1.2.2, or (c) withdraw the proposed amendments. The PMA is entitled to withdraw proposed amendments by notifying Affiliates and providing notice in the Practices Updates and Notices section of the VeriSign Repository. Unless proposed amendments are amended or withdrawn, they shall become effective upon the expiration of the comment period under Section 8.1.2.3.

8.1.3 Changes Requiring Changes in the Certificate Policy OID or CPS Pointer

If the PMA determines that a change is necessary in the object identifier corresponding to a Certificate policy, the amendment shall contain new object identifiers for the Certificate policies

corresponding to each Class of Certificate. Otherwise, amendments shall not require a change in Certificate policy object identifier.

8.2 Publication and Notification Policies

8.2.1 Items Not Published in the CP

Security documents and information in them considered confidential by VeriSign and the Affiliates are not disclosed to the public. Confidential security documents include the documents identified in CP § 1.1(a) Table 1 as documents that are not available to the public.

8.2.2 Distribution of the CP

This CP is published in electronic form within the VeriSign Repository at <https://www.verisign.com/CP>. The CP is available in paper form from the PMA upon requests sent to: VeriSign, Inc., 487 E. Middlefield Road, Mountain View, CA 94043 USA, Attn: Practices and External Affairs – CP.

8.3 CPS Approval Procedures

VTN Affiliates shall each have their own CPS. An Affiliate’s CPSs will govern the Affiliate’s Subdomain within the VTN. Entities wishing to become Affiliates sign an agreement with VeriSign and submit a proposed CPS to the Practices and External Affairs Department of VeriSign. The Practices and External Affairs Department shall approve or reject the CPSs proposed by potential Affiliates within its sole discretion. See CP § 1.4.2 for the contact information for the Practices and External Affairs Department.

Acronyms and Definitions

Table of Acronyms

Acronym	Term
ANSI	The American National Standards Institute.
ASB	Authentication Service Bureau.
B2B	Business-to-business.
BIS	The United States Bureau of Industry and Science of the United States Department of Commerce.
BXA	The United States Bureau of Export Administration of the United States Department of Commerce (which has been replaced by the BIS).
CA	Certification Authority.
CP	Certificate Policy.
CPS	Certification Practice Statement.
CRL	Certificate Revocation List.
EAL	Evaluation assurance level (pursuant to the Common Criteria).
EDI	Electronic Data Interchange.
EDIFACT	EDI for Administration, Commerce, and Transport (standards established by the

Acronym	Term
	United Nations Economic Commission for Europe).
FIPS	United State Federal Information Processing Standards.
ICC	International Chamber of Commerce.
KRB	Key Recovery Block.
LSVA	Logical security vulnerability assessment.
OCSP	Online Certificate Status Protocol.
OFX	Open Financial Exchange.
PCA	Primary Certification Authority.
PIN	Personal identification number.
PKCS	Public-Key Cryptography Standard.
PKI	Public Key Infrastructure.
PMA	Policy Management Authority.
RA	Registration Authority.
RFC	Request for comment.
SAS	Statement on Auditing Standards (promulgated by the American Institute of Certified Public Accountants).
S/MIME	Secure multipurpose Internet mail extensions.
SSL	Secure Sockets Layer.
VTN	VeriSign Trust Network.
WAP	Wireless Application Protocol.
WTLS	Wireless Transport Layer Security.

Definitions

Term	Definition
Administrator	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.
Administrator Certificate	A Certificate issued to an Administrator that may only be used to perform CA or RA functions.
Affiliate	A leading trusted third party, for example in the technology, telecommunications, or financial services industry, that has entered into an agreement with VeriSign to be a VTN distribution and services channel within a specific territory.
Affiliate Audit Program Guide	A VeriSign document containing requirements for the Compliance Audits of Affiliates, including Certificate Management Control Objectives against which Affiliates will be audited.
Affiliate Practices Legal Requirements Guidebook	A VeriSign document setting forth requirements for Affiliate CPSs, agreements, validation procedures, and privacy policies, as well as other requirements that Affiliates must meet.
Affiliated Individual	A natural person that is related to a Managed PKI Customer,

Term	Definition
	Managed PKI Lite Customer, or Gateway Customer entity (i) as an officer, director, employee, partner, contractor, intern, or other person within the entity, (ii) as a member of a VeriSign registered community of interest, or (iii) as a person maintaining a relationship with the entity where the entity has business or other records providing appropriate assurances of the identity of such person.
<i>ASB Customer</i>	An entity that contracts with VeriSign or an Affiliate to obtain Authentication Service Bureau services. An ASB Customer is a CA, and is named as such within the Certificates issued by its CA, but it outsources all CA functions to an ASB Provider.
<i>ASB Provider</i>	An entity (either VeriSign or an Affiliate) that offers Authentication Service Bureau services to ASB Customers. An ASB Provider acts as an outsourcing provider of back-end functions for an ASB Customer and as an RA for the ASB Customer.
<i>Authentication Service Bureau</i>	A service within the VTN by which VeriSign or an Affiliate performs most front-end RA and all back-end CA functions on behalf of an organization.
<i>Automated Administration</i>	A procedure whereby Certificate Applications are approved automatically if enrollment information matches information contained in a database.
<i>Automated Administration Software Module</i>	Software provided by VeriSign that performs Automated Administration.
<i>Certificate</i>	A message that, at least, states a name or identifies the CA, identifies the Subscriber, contains the Subscriber's public key, identifies the Certificate's Operational Period, contains a Certificate serial number, and is digitally signed by the CA.
<i>Certificate Applicant</i>	An individual or organization that requests the issuance of a Certificate by a CA.
<i>Certificate Application</i>	A request from a Certificate Applicant (or authorized agent of the Certificate Applicant) to a CA for the issuance of a Certificate.
<i>Certificate Chain</i>	An ordered list of Certificates containing an end-user Subscriber Certificate and CA Certificates, which terminates in a root Certificate.
<i>Certificate Management Control Objectives</i>	Criteria that an entity must meet in order to satisfy a Compliance Audit.
<i>Certificate Policies (CP)</i>	This document, which is entitled "VeriSign Trust Network Certificate Policies" and is the principal statement of policy governing the VTN.
<i>Certificate Revocation List (CRL)</i>	A periodically (or exigently) issued list, digitally signed by a CA, of identified Certificates that have been revoked prior to their expiration dates in accordance with CP § 3.4. 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,

Term	Definition
	and the specific times and reasons for revocation.
<i>Certificate Signing Request</i>	A message conveying a request to have a Certificate issued.
<i>Certification Authority (CA)</i>	An entity authorized to issue, manage, revoke, and renew Certificates in the VTN.
<i>Certification Practice Statement (CPS)</i>	A statement of the practices that VeriSign or an Affiliate employs in approving or rejecting Certificate Applications and issuing, managing, and revoking Certificates, and requires its Managed PKI Customers and Gateway Customers to employ.
<i>Challenge Phrase</i>	A secret phrase chosen by a Certificate Applicant during enrollment for a Certificate. When issued a Certificate, the Certificate Applicant becomes a Subscriber and a CA or RA can use the Challenge Phrase to authenticate the Subscriber when the Subscriber seeks to revoke or renew the Subscriber's Certificate.
<i>Class</i>	A specified level of assurances as defined within the CP. See CP § 1.1.1.
<i>Class 2 Individual ASB Certificate</i>	A Class 2 individual Certificate issued by an ASB Provider on behalf of an ASB Customer CA.
<i>Class 3 Organizational ASB Certificate</i>	A Class 3 organizational Certificate issued by an ASB Provider on behalf of an ASB Customer CA.
<i>Client OnSite Lite Customer</i>	See Managed PKI Lite Customer.
<i>Client Service Center</i>	A Service Center that is an Affiliate providing client Certificates either in the Consumer or Enterprise line of business.
<i>Compliance Audit</i>	A periodic audit that a Processing Center, Service Center, Managed PKI Customer, or Gateway Customer undergoes to determine its conformance with VTN Standards that apply to it.
<i>Compromise</i>	A violation (or suspected violation) of a security policy, in which an unauthorized disclosure of, or loss of control over, sensitive information may have occurred. With respect to private keys, a Compromise is a loss, theft, disclosure, modification, unauthorized use, or other compromise of the security of such private key.
<i>Confidential/Private Information</i>	Information required to be kept confidential and private pursuant to CP § 2.8.1.
<i>Consumer, as in Consumer Service Center</i>	A line of business that an Affiliate enters to provide client Retail Certificates to Certificate Applicants.
<i>CRL Usage Agreement</i>	An agreement setting forth the terms and conditions under which a CRL or the information in it can be used.
<i>Customer</i>	An organization that is either a Managed PKI Customer, Gateway Customer, or ASB Customer.
<i>Digital Receipt</i>	A data object created in connection with the VeriSign Digital Notarization Service and digitally signed by the Time-Stamping

Term	Definition
	Authority that includes the hash of a document or set of data and a time-stamp showing that the document or data existed at a certain time.
Electronic Data Interchange (EDI)	The computer-to-computer exchange of business transactions, such as purchase orders, invoices, and payment advices in accordance with applicable standards.
Electronic Data Interchange Certificate (EDI Certificate)	A Class 3 organizational Certificate that allows for digital signatures on Electronic Data Interchange messages and for the encryption of EDI messages. ³
Enterprise, as in Enterprise Service Center	A line of business that an Affiliate enters to provide Managed PKI services to Managed PKI Customers.
Enterprise Roaming Server	A server residing at the site of a Managed PKI Customer used in conjunction with the VeriSign Roaming Service to hold Roaming Subscribers' encrypted private keys and portions of symmetric keys used to encrypt and decrypt Roaming Subscribers' private keys.
Enterprise Security Guide	A document setting forth security recommendations for Managed PKI Customers and Gateway Customers.
Exigent Audit/Investigation	An audit or investigation by VeriSign where VeriSign has reason to believe that an entity's failure to meet VTN Standards, an incident or Compromise relating to the entity, or an actual or potential threat to the security of the VTN posed by the entity has occurred.
Gateway	A service offered by VeriSign or an Affiliate to allow an organization using a stand-alone Certificate server to become a CA within the VTN by having a VeriSign CA certify the organization's public key.
Gateway Administrator	An Administrator that performs validation or other RA functions for a Gateway Customer.
Gateway Certificate	A Certificate issued to a Gateway Customer certifying its public key.
Gateway Customer	An organization that has obtained Gateway services from VeriSign or an Affiliate, whereby the organization becomes a CA within the VTN to issue Class 1 Certificates.
Global Server ID	A Class 3 organizational Certificate used to support SSL sessions between web browsers and web servers that are encrypted using strong cryptographic protection consistent with applicable export laws.
Global Server OnSite	See Managed PKI for SSL Premium Edition.
Global Server OnSite Customer	See Managed PKI for SSL Premium Edition Customer.
Go Secure!	A suite of plug-and-play services building on Managed PKI services and designed to accelerate e-commerce applications.

³ EDI certificates are no longer part of Verisign's service offering

Term	Definition
<i>Intellectual Property Rights</i>	Rights under one or more of the following: any copyright, patent, trade secret, trademark, and any other intellectual property rights.
<i>Intermediate Certification Authority (Intermediate CA)</i>	A Certification Authority whose Certificate is located within a Certificate Chain between the Certificate of the root CA and the Certificate of the Certification Authority that issued the end-user Subscriber's Certificate.
<i>Key Ceremony Reference Guide</i>	A document describing Key Generation Ceremony requirements and practices.
<i>Key Generation Ceremony</i>	A procedure whereby a CA's or RA's key pair is generated, its private key is transferred into a cryptographic module, its private key is backed up, and/or its public key is certified.
<i>Key Manager Administrator</i>	An Administrator that performs key generation and recovery functions for a Managed PKI Customer using Managed PKI Key Manager.
<i>Key Recovery Block (KRB)</i>	A data structure containing a Subscriber's private key that is encrypted using an encryption key. KRBs are generated using Managed PKI Key Manager software.
<i>Key Recovery Service</i>	A VeriSign service that provides encryption keys needed to recover a Key Recovery Block as part of a Managed PKI Customer's use of Managed PKI Key Manager to recover a Subscriber's private key.
<i>Managed PKI</i>	VeriSign's fully integrated managed PKI service that allows enterprise Customers of VeriSign and its Affiliates to distribute Certificates to individuals, such as employees, partners, suppliers, and customers, as well as devices, such as servers, routers, and firewalls. Managed PKI permits enterprises to secure messaging, intranet, extranet, virtual private network, and e-commerce applications.
<i>Managed PKI Administrator</i>	An Administrator that performs validation or other RA functions for an Managed PKI Customer.
<i>Managed PKI Administrator's Handbook</i>	A VeriSign document setting forth the operational requirements and practices for Managed PKI Customers.
<i>Managed PKI Agreement</i>	An agreement under which an organization becomes an Managed PKI Customer and agrees to be bound by VeriSign's or an Affiliate's CPS.
<i>Managed PKI Certificate</i>	A Certificate whose Certificate Application was approved by a Managed PKI Customer.
<i>Managed PKI Customer</i>	An organization that has obtained Managed PKI services from VeriSign or an Affiliate, whereby the organization becomes a CA within the VTN to issue client and/or server Certificates. Managed PKI Customers outsource back-end functions of issuance, management, and revocation to VeriSign or the Affiliate, but retain for themselves the RA functions of approving or rejecting Certificate Applications and initiating revocations and renewals of

Term	Definition
	Certificates.
Managed PKI Control Center	A web-based interface that permits Managed PKI Administrators to perform Manual Authentication of Certificate Applications
Managed PKI Key Manager	A key recovery solution for those Managed PKI Customers choosing to implement key recovery under a special Managed PKI Agreement.
Managed PKI Key Management Service Administrator's Guide	A document setting forth the operational requirements and practices for Managed PKI Customers using Managed PKI Key Manager.
Managed PKI Lite	A type of Managed PKI service that permits an organization to become a Registration Authority within the VTN to assist a VeriSign or Affiliate CA to issue client Certificates.
Managed PKI for SSL	A type of Managed PKI service that permits an organization to become an RA within the VTN to assist a VeriSign or Affiliate CA to issue Secure Server IDs within designated domains. This CA delegates to Server Managed PKI Customers the RA functions of approving or rejecting Certificate Applications and initiating revocations and renewals of Secure Server IDs.
Managed PKI for SSL Customer	An organization that has obtained Managed PKI for SSL services from VeriSign or an Affiliate.
Managed PKI for SSL Premium Edition	A type of Managed PKI service that permits an organization to become an RA within the VTN to assist a VeriSign or Affiliate CA to issue Global Server IDs within designated domains. This CA delegates to Managed PKI for SSL Premium Edition Customers the RA functions of approving or rejecting Certificate Applications and initiating revocations and renewals of Global Server IDs.
Managed PKI for SSL Premium Edition Customer	An organization that has obtained Managed PKI for SSL Premium Edition services from VeriSign or an Affiliate
Managed PKI Lite Customer	An organization that has obtained Managed PKI Lite services from VeriSign or an Affiliate, whereby the organization becomes a Registration Authority within the VTN to assist a VeriSign or Affiliate CA to issue client Certificates. This CA delegates to Managed PKI Lite Customers the RA functions of approving or rejecting Certificate Applications and initiating revocations and renewals of Certificates.
Manual Authentication	A procedure whereby Certificate Applications are reviewed and approved manually one-by-one by an Administrator using a web-based interface.
NetSure Protection Plan	An extended warranty program, which is described in CP § 1.1.2.2.3.
Nonverified Subscriber Information	Information submitted by a Certificate Applicant to a CA or RA, and included within a Certificate, that has not been confirmed by the CA or RA and for which the applicable CA and RA provide no

Term	Definition
	assurances other than that the information was submitted by the Certificate Applicant.
<i>Non-repudiation</i>	An attribute of a communication that provides protection against a party to a communication falsely denying its origin, denying that it was submitted, or denying its delivery. Denial of origin includes the denial that a communication originated from the same source as a sequence of one or more prior messages, even if the identity associated with the sender is unknown. Note: only an adjudication by a court, arbitration panel, or other tribunal can ultimately prevent repudiation. For example, a digital signature verified with reference to a VTN Certificate may provide proof in support of a determination of Non-repudiation by a tribunal, but does not by itself constitute Non-repudiation.
<i>OFX Certificate</i>	A Class 3 organizational Certificate issued to a financial institution's server for use with the Open Financial Exchange specification.
<i>Online Certificate Status Protocol (OCSP)</i>	A protocol for providing Relying Parties with real-time Certificate status information.
<i>OnSite</i>	See Managed PKI.
<i>OnSite Administrator</i>	See Managed PKI Administrator.
<i>OnSite Administrator's Handbook</i>	See Managed PKI Administrator's Handbook.
<i>OnSite Agreement</i>	See Managed PKI Agreement.
<i>OnSite Certificate</i>	Managed PKI Certificate.
<i>OnSite Control Center</i>	Managed PKI Control Center.
<i>OnSite Customer</i>	See Managed PKI Customer.
<i>OnSite Key Manager</i>	See Managed PKI Key Manager.
<i>OnSite Key Management Service Administrator's Guide</i>	See Managed PKI Key Management Service Administrator's Guide.
<i>OnSite Lite</i>	See Managed PKI Lite.
<i>Open Financial Exchange (OFX)</i>	A standard web-based specification for the electronic exchange of financial data among financial institutions, businesses, and consumers.
<i>Operational Period</i>	The period starting with the date and time a Certificate is issued (or on a later date and time certain if stated in the Certificate) and ending with the date and time on which the Certificate expires or is earlier revoked.
<i>PKCS #10</i>	Public-Key Cryptography Standard #10, developed by RSA Security Inc., which defines a structure for a Certificate Signing Request.
<i>PKCS #12</i>	Public-Key Cryptography Standard #12, developed by RSA

Term	Definition
	Security Inc., which defines a secure means for the transfer of private keys.
Policy Management Authority (PMA)	The organization within VeriSign responsible for promulgating this policy throughout the VTN.
Primary Certification Authority (PCA)	A CA that acts as a root CA for a specific Class of Certificates, and issues Certificates to CAs subordinate to it.
Processing Center	An organization (VeriSign or certain Affiliates) that creates a secure facility housing, among other things, the cryptographic modules used for the issuance of Certificates. In the Consumer and Web Site lines of business, Processing Centers act as CAs within the VTN and perform all Certificate lifecycle services of issuing, managing, revoking, and renewing Certificates. In the Enterprise line of business, Processing Centers provide lifecycle services on behalf of their Managed PKI Customers or the Managed PKI Customers of the Service Centers subordinate to them.
Public Key Infrastructure (PKI)	The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a Certificate-based public key cryptographic system. The VTN PKI consists of systems that collaborate to provide and implement the VTN.
Registration Authority (RA)	An entity approved by a CA to assist Certificate Applicants in applying for Certificates, and to approve or reject Certificate Applications, revoke Certificates, or renew Certificates.
Relying Party	An individual or organization that acts in reliance on a certificate and/or a digital signature.
Relying Party Agreement	An agreement used by a CA setting forth the terms and conditions under which an individual or organization acts as a Relying Party.
Retail Certificate	A Certificate issued by VeriSign or an Affiliate, acting as CA, to individuals or organizations applying one by one to VeriSign or an Affiliate on its web site.
Roaming Subscriber	A Subscriber using the VeriSign Roaming Service whose private key is encrypted and decrypted with a symmetric key that is split between the VeriSign Roaming Server and an Enterprise Roaming Server.
RSA	A public key cryptographic system invented by Rivest, Shamir, and Adelman.
RSA Secure Server Certification Authority (RSA Secure Server CA)	The Certification Authority that issues Secure Server IDs.
RSA Secure Server Hierarchy	The PKI hierarchy comprised of the RSA Secure Server Certification Authority.
Secret Share	A portion of a CA private key or a portion of the activation data needed to operate a CA private key under a Secret Sharing

Term	Definition
	arrangement.
<i>Secret Sharing</i>	The practice of splitting a CA private key or the activation data to operate a CA private key in order to enforce multi-person control over CA private key operations under CP § 6.2.2.
<i>Secure Server ID</i>	A Class 3 organizational Certificate used to support SSL sessions between web browsers and web servers.
<i>Secure Sockets Layer (SSL)</i>	The industry-standard method for protecting Web communications developed by Netscape Communications Corporation. The SSL security protocol provides data encryption, server authentication, message integrity, and optional client authentication for a Transmission Control Protocol/Internet Protocol connection.
<i>Security and Audit Requirements Guide</i>	A VeriSign document that sets forth the security and audit requirements and practices for Processing Centers and Service Centers.
<i>Security and Practices Review</i>	A review of an Affiliate performed by VeriSign before an Affiliate is permitted to become operational.
<i>Server Gated Cryptography</i>	A technology that permits web servers that have been issued a Global Server ID to create an SSL session with a browser that is encrypted using strong cryptographic protection.
<i>Server OnSite</i>	See Managed PKI for SSL.
<i>Server OnSite Customer</i>	See Managed PKI for SSL Customer.
<i>Server Service Center</i>	A Service Center that is an Affiliate providing Secure Server IDs and Global Server IDs either in the Web Site or Enterprise line of business.
<i>Service Center</i>	An Affiliate that does not house Certificate signing units for the issuance of Certificates for the purpose of issuing Certificates of a specific Class or type, but rather relies on a Processing Center to perform issuance, management, revocation, and renewal of such Certificates.
<i>Subdomain</i>	The portion of the VTN under control of an entity and all entities subordinate to it within the VTN hierarchy.
<i>Subject</i>	The holder of a private key corresponding to a public key. The term "Subject" can, in the case of an organizational Certificate, refer to the equipment or device that holds a private key. A Subject is assigned an unambiguous name, which is bound to the public key contained in the Subject's Certificate.
<i>Subscriber</i>	In the case of an individual Certificate, a person who is the Subject of, and has been issued, a Certificate. In the case of an organizational Certificate, an organization that owns the equipment or device that is the Subject of, and that has been issued, a Certificate. 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	Definition
<i>Subscriber Agreement</i>	An agreement used by a CA or RA setting forth the terms and conditions under which an individual or organization acts as a Subscriber.
<i>Superior Entity</i>	An entity above a certain entity within a VTN hierarchy (the Class 1, 2, or 3 hierarchy).
<i>Supplemental Risk Management Review</i>	A review of an entity by VeriSign following incomplete or exceptional findings in a Compliance Audit of the entity or as part of the overall risk management process in the ordinary course of business.
<i>Reseller</i>	An entity marketing services on behalf of VeriSign or an Affiliate to specific markets.
<i>Time-Stamping Authority</i>	The VeriSign entity that signs Digital Receipts as part of the VeriSign Digital Notarization Service.
<i>Time-Stamping Authority CA</i>	The VeriSign CA that issued a special Class 3 organizational Certificate to the Time-Stamping Authority used to verify the digital signatures on Digital Receipts.
<i>Trusted Person</i>	An employee, contractor, or consultant of an entity within the VTN responsible for managing infrastructural trustworthiness of the entity, its products, its services, its facilities, and/or its practices as further defined in CP § 5.2.1.
<i>Trusted Position</i>	The positions within a VTN entity that must be held by a Trusted Person.
<i>Trustworthy System</i>	Computer hardware, software, and procedures that are reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy. A trustworthy system is not necessarily a “trusted system” as recognized in classified government nomenclature.
<i>Universal Service Center</i>	An entity participating in the Universal Service Center Program.
<i>Universal Service Center Program</i>	A program by which entities market VeriSign’s services to specific markets using a specialized software platform for managing complex, multi-tiered PKI deployment.
<i>VeriSign</i>	Means, with respect to each pertinent portion of this CPS, VeriSign, Inc. and/or any wholly owned VeriSign subsidiary responsible for the specific operations at issue.
<i>VeriSign Digital Notarization Service</i>	A service offered to Managed PKI Customers that provides a digitally signed assertion (a Digital Receipt) that a particular document or set of data existed at a particular point in time.
<i>VeriSign Repository</i>	VeriSign’s database of Certificates and other relevant VeriSign Trust Network information accessible on-line.
<i>VeriSign Roaming Server</i>	A server residing at VeriSign’s Processing Center used in conjunction with the VeriSign Roaming Service to hold portions of symmetric keys used to encrypt and decrypt Roaming Subscribers’

Term	Definition
	private keys.
VeriSign Roaming Service	The service offered by VeriSign that enables a Subscriber to download his or her private key and perform private key operations on different client terminals.
VeriSign Physical Security Policy	The highest-level document describing VeriSign's security policies.
VeriSign Trust Network (VTN)	The Certificate-based Public Key Infrastructure governed by the VeriSign Trust Network Certificate Policies, which enables the worldwide deployment and use of Certificates by VeriSign and its Affiliates, and their respective Customers, Subscribers, and Relying Parties.
VTN Participant	An individual or organization that is one or more of the following within the VTN: VeriSign, an Affiliate, a Customer, a Universal Service Center, a Reseller, a Subscriber, or a Relying Party.
VTN Standards	The business, legal, and technical requirements for issuing, managing, revoking, renewing, and using Certificates within the VTN.
Web Host	An entity hosting the web site of another, such as an Internet service provider, a systems integrator, a Reseller, a technical consultant, and application service provider, or similar entity.
Web Host Program	A program that allows Web Hosts to enroll for Secure Server IDs and Global Server IDs on behalf of end-user Subscribers who are customers of the Web Hosts.
Web Site, as in Web Site Service Center	A line of business that an Affiliate enters to provide Secure Server ID and Global Server ID Retail Certificates one by one to Certificate Applicants.
Wireless Application Protocol (WAP)	A standard for the presentation and delivery of wireless information and telephony services on mobile phones and other wireless terminals.
Wireless Transport Layer Security (WTLS)	A protocol that protects the communication of applications that operate using the Wireless Application Protocol, such as communications between a wireless handset and a server.
Wireless Transport Layer Security Certificate (WTLS Certificate)	A Class 3 organizational Certificate whose format is defined as part of the Wireless Application Protocol, which authenticates a Wireless Transport Layer Security server to a WTLS client and facilitates encrypted communication between the WTLS server and the WTLS client.