

VeriSign  
DOD IECA  
Certification  
Practices  
Statement

Version 3.0

February 2002

Copyright © 2000 VeriSign, Inc. All Rights Reserved

## Table of Contents

<b>1.</b>	<b>INTRODUCTION.....</b>	<b>7</b>
1.1	OVERVIEW.....	7
1.2	POLICY IDENTIFICATION.....	10
1.3	COMMUNITY AND APPLICABILITY .....	10
1.3.1	<i>CMI Authorities</i> .....	11
1.3.1.1	Certificate Authority (CA).....	11
1.3.1.2	Registration Authority (RA).....	12
1.3.1.3	Repository.....	12
1.3.2	<i>Related Authorities</i> .....	12
1.3.2.1	Notaries.....	12
1.3.2.2	Affiliated Company.....	13
1.3.2.3	Auditor.....	13
1.3.2.4	Policy Authority.....	14
1.3.3	<i>End-Entities</i> .....	14
1.3.3.1	Subscribers.....	14
1.3.3.2	Relying Parties.....	14
1.3.4	<i>Applicability</i> .....	14
1.4	CONTACT DETAILS.....	15
1.4.1	<i>Specification Administration Organization</i> .....	15
1.4.2	<i>Contact Persons</i> .....	15
1.4.3	<i>Person Determining CPS Suitability for the Policy</i> .....	15
<b>2.</b>	<b>GENERAL PROVISIONS.....</b>	<b>16</b>
2.1	OBLIGATIONS.....	16
2.1.1	<i>CA Obligations</i> .....	16
2.1.2	<i>RA Obligations</i> .....	17
2.1.3	<i>Subscriber Obligations</i> .....	17
2.1.4	<i>Relying Party Obligations</i> .....	18
2.1.5	<i>Repository Obligations</i> .....	19
2.2	LIABILITY.....	19
2.2.1	<i>Warranties and Limitations on Warranties</i> .....	19
2.2.1.1	CA Warranties.....	19
2.2.1.1.1	Scope of the NetSure <sup>SM</sup> Protection Plan.....	19
2.2.1.1.1.1	Who is Covered.....	19
2.2.1.1.1.2	When the Coverage Applies.....	20
2.2.1.1.2	What is covered.....	21
2.2.1.1.3	Payments and Payment Requests.....	22
2.2.1.1.4	Limitations on Payments.....	23
2.2.1.1.5	Persons Excluded from Protections.....	25
2.2.1.1.6	Exceptions to Limited Warranties.....	25
2.2.1.2	RA Warranties.....	26
2.2.1.3	Subscribers' Representations.....	26
2.2.1.3.1	General Representations.....	26
2.2.1.3.2	Representations Relating to Intellectual Property Infringement.....	27
2.2.2	<i>Disclaimers of Warranty and Liability</i> .....	28
2.2.2.1	<b>SPECIFIC DISCLAIMERS</b> .....	28
2.2.2.2	<b>GENERAL DISCLAIMER</b> .....	28
2.2.3	<i>Limitations of Liability</i> .....	29
2.2.3.1	<b>LIMITATIONS ON AMOUNT OF DAMAGES</b> .....	29
2.2.3.2	<b>EXCLUSION OF CERTAIN ELEMENTS OF DAMAGES</b> .....	30
2.3	FINANCIAL RESPONSIBILITY.....	30
2.3.1	<i>Subscriber's Liability and Indemnity</i> .....	30
2.3.2	<i>Fiduciary Relationships</i> .....	31
2.3.3	<i>Administrative Processes</i> .....	31
2.4	INTERPRETATION AND ENFORCEMENT .....	31
2.4.1	<i>Interpretation</i> .....	31

2.4.1.1	Governing Law.....	31
2.4.1.2	Conflict of Provisions.....	32
2.4.1.3	Interpretation.....	32
2.4.1.4	Headings and Appendices of this CPS.....	32
2.4.2	<i>Severability, Survival, Merger, and Notice</i> .....	32
2.4.2.1	Severability.....	32
2.4.2.2	Survival.....	33
2.4.2.3	Merger.....	33
2.4.2.4	Notice.....	33
2.4.3	<i>Dispute Resolution Procedures and Choice of Forum</i> .....	34
2.4.3.1	Notification Among Parties to a Dispute.....	34
2.4.3.2	Formal Dispute Resolution.....	34
2.4.4	<i>Successors and Assigns</i> .....	35
2.4.5	<i>No Waiver</i> .....	35
2.4.6	<i>Compliance with Export Laws and Regulations</i> .....	35
2.4.7	<i>Choice of Cryptographic Methods</i> .....	35
2.4.8	<i>Force Majeure</i> .....	35
2.5	FEES.....	36
2.5.1	<i>Certificate Issuance or Renewal Fees</i> .....	36
2.5.2	<i>Certificate Access Fees</i> .....	36
2.5.3	<i>Revocation or Status Information Access Fees</i> .....	36
2.5.4	<i>Fees for Other Services</i> .....	36
2.5.5	<i>Refund Policy</i> .....	36
2.6	PUBLICATION AND REPOSITORIES.....	36
2.6.1	<i>Publication of CA Information</i> .....	36
2.6.2	<i>Frequency of Publication</i> .....	37
2.6.3	<i>Access Controls</i> .....	37
2.6.4	<i>Repositories</i> .....	37
2.7	COMPLIANCE AUDIT.....	38
2.7.1	<i>Frequency of Compliance Audit</i> .....	38
2.7.2	<i>Identity/Qualifications of Reviewer</i> .....	38
2.7.3	<i>Auditor's Relationship to Audited Party</i> .....	38
2.7.4	<i>Topics Covered by Audit</i> .....	38
2.7.5	<i>Actions Taken as a Result of Deficiency</i> .....	39
2.7.6	<i>Communication of Results</i> .....	39
2.8	CONFIDENTIALITY.....	39
2.8.1	<i>Types of Information to Be Kept Confidential</i> .....	39
2.8.2	<i>Types of Information Not Considered Confidential</i> .....	40
2.8.3	<i>Disclosure of Certificate Revocation/Suspension Information</i> .....	40
2.8.4	<i>Release to Law Enforcement Officials</i> .....	40
2.8.5	<i>Release as Part of Civil Discovery</i> .....	40
2.8.6	<i>Disclosure upon Owner's Request</i> .....	40
2.8.7	<i>Other Information Release Circumstances</i> .....	40
2.9	INTELLECTUAL PROPERTY RIGHTS.....	40
<b>3.</b>	<b>IDENTIFICATION AND AUTHENTICATION.....</b>	<b>42</b>
3.1	INITIAL REGISTRATION.....	42
3.1.1	<i>Types of Names</i> .....	42
3.1.2	<i>Need for Names to be Meaningful</i> .....	42
3.1.3	<i>Rules for Interpreting Various Name Forms</i> .....	42
3.1.4	<i>Uniqueness of Names</i> .....	42
3.1.5	<i>Name Claim Dispute Procedure</i> .....	42
3.1.6	<i>Recognition, authentication, and role of trademarks</i> .....	42
3.1.7	<i>Method to prove possession of private key</i> .....	43
3.1.8	<i>Authentication of individual identity</i> .....	43
3.2	CERTIFICATE RENEWAL, UPDATE, AND ROUTINE RE-KEY.....	43
3.2.1	<i>Certificate re-key</i> .....	43
3.2.2	<i>Certificate renewal</i> .....	44

3.2.3	<i>Certificate update</i> .....	44
3.3	RE-KEY AFTER REVOCATION.....	44
3.4	REVOCATION REQUEST.....	44
<b>4</b>	<b>OPERATIONAL REQUIREMENTS.....</b>	<b>45</b>
4.1	CERTIFICATE APPLICATION .....	45
4.2	CERTIFICATE ISSUANCE .....	46
4.3	CERTIFICATE ACCEPTANCE.....	46
4.4	CERTIFICATE SUSPENSION AND REVOCATION .....	47
4.4.1	<i>Revocation</i> .....	47
4.4.1.1	Circumstances for Revocation.....	47
4.4.1.2	Who Can Request Revocation.....	47
4.4.1.3	Procedure for Revocation Request.....	47
4.4.1.4	Revocation Request Grace Period.....	48
4.4.2	<i>Suspension</i> .....	48
4.4.3	<i>Certificate Revocation Lists</i> .....	48
4.4.3.1	CRL Issuance Frequency.....	48
4.4.3.2	CRL Checking Requirements.....	48
4.4.4	<i>Online Status Checking</i> .....	48
4.4.5	<i>Other Forms of Revocation Advertisements Available</i> .....	48
4.4.6	<i>Special Requirements Related to Key Compromise</i> .....	48
4.5	SECURITY AUDIT PROCEDURES.....	49
4.5.1	<i>Types of Events Recorded</i> .....	49
4.5.2	<i>Frequency of Processing Log</i> .....	51
4.5.3	<i>Retention Period of Audit Log</i> .....	51
4.5.4	<i>Protection of Audit Log</i> .....	51
4.5.5	<i>Audit Log backup Procedures</i> .....	52
4.5.6	<i>Audit Collection System</i> .....	52
4.5.7	<i>Notification to Event-Causing Subject</i> .....	52
4.5.8	<i>Vulnerability Assessments</i> .....	52
4.6	RECORDS ARCHIVAL.....	53
4.6.1	<i>Types of Data Archived</i> .....	53
4.6.2	<i>Retention Period for Archive</i> .....	53
4.6.3	<i>Protection of Archive</i> .....	53
4.6.4	<i>Archive Backup Procedures</i> .....	54
4.6.5	<i>Archive Collection System</i> .....	54
4.6.6	<i>Procedures to Obtain and Verify Archive Information</i> .....	54
4.7	KEY CHANGEOVER.....	54
4.8	COMPROMISE AND DISASTER RECOVERY.....	55
4.8.1	<i>Compromise recovery</i> .....	55
4.8.2	<i>Disaster Recovery</i> .....	55
4.8.2.1	Disaster Recovery Process Initialization.....	55
4.8.2.2	VeriSign Disaster Recovery Infrastructure.....	56
4.8.2.3	Disaster Recovery At Time of Disaster (Hotsite).....	56
4.9	CA TERMINATION .....	56
<b>5</b>	<b>PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS.....</b>	<b>58</b>
5.1	PHYSICAL CONTROLS.....	58
5.1.1	<i>Site Location and Construction</i> .....	58
5.1.2	<i>Physical Access</i> .....	58
5.1.3	<i>Power and Air Conditioning</i> .....	59
5.1.4	<i>Water Exposure</i> .....	60
5.1.5	<i>Fire Prevention and Protection</i> .....	60
5.1.6	<i>Media Storage</i> .....	60
5.1.7	<i>Waste Disposal</i> .....	60
5.1.8	<i>Off-Site Backup</i> .....	60
5.2	PROCEDURAL CONTROLS.....	60
5.2.1	<i>Trusted Roles</i> .....	60

5.2.2	<i>Number of Persons Required Per Task</i> .....	62
5.3	PERSONNEL SECURITY CONTROLS.....	63
5.3.1	<i>Background, Qualifications, Experience and Clearance Requirements</i> .....	63
5.3.2	<i>Background Check Procedures</i> .....	64
5.3.3	<i>Training Requirements</i> .....	64
5.3.4	<i>Retraining Frequency and Requirements</i> .....	65
5.3.5	<i>Job Rotation Frequency and Sequence</i> .....	65
5.3.6	<i>Sanctions for Unauthorized Actions</i> .....	65
5.3.7	<i>Contracting Personnel Requirements</i> .....	65
5.3.8	<i>Documentation Supplied to Personnel</i> .....	65
<b>6</b>	<b>TECHNICAL SECURITY CONTROLS</b> .....	<b>66</b>
6.1	KEY PAIR GENERATION AND INSTALLATION.....	66
6.1.1	<i>Key Pair Generation</i> .....	66
6.1.2	<i>Private Key Delivery to Entity</i> .....	66
6.1.3	<i>Public Key Delivery to certificate issuer</i> .....	66
6.1.4	<i>CA Public Key Delivery to Users</i> .....	66
6.1.5	<i>Key Sizes</i> .....	66
6.1.6	<i>Public Key Parameters</i> .....	66
6.1.7	<i>Parameter quality checking</i> .....	67
6.1.8	<i>Hardware/software key generation</i> .....	67
6.1.9	<i>Key usage purposes</i> .....	67
6.2	CA PRIVATE KEY PROTECTION.....	67
6.2.1	<i>Standards for cryptographic modules</i> .....	67
6.2.2	<i>Private key multi-person control</i> .....	67
6.2.3	<i>Private key escrow</i> .....	68
6.2.4	<i>Private key backup</i> .....	68
6.2.5	<i>Private key archival</i> .....	69
6.2.6	<i>Private key entry into cryptographic module</i> .....	69
6.2.7	<i>Method of activating private key</i> .....	69
6.2.8	<i>Method of deactivating private key</i> .....	69
6.2.9	<i>Method of destroying private key</i> .....	69
6.3	OTHER ASPECTS OF KEY PAIR MANAGEMENT.....	69
6.3.1	<i>Public Key Archival</i> .....	69
6.3.2	<i>Usage Periods for the Public and Private Keys (Key Replacement)</i> .....	70
6.4	ACTIVATION DATA.....	70
6.4.1	<i>Activation data generation and installation</i> .....	70
6.4.2	<i>Activation data protection</i> .....	70
6.4.3	<i>Other aspects of activation data</i> .....	70
6.5	COMPUTER SECURITY CONTROLS.....	70
6.5.1	<i>Specific computer security technical requirements</i> .....	70
6.5.2	<i>Computer security rating</i> .....	71
6.6	LIFE CYCLE TECHNICAL CONTROLS.....	71
6.7	NETWORK SECURITY CONTROLS.....	71
6.8	CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS.....	72
<b>7</b>	<b>CERTIFICATE AND CRL PROFILES</b> .....	<b>73</b>
7.1	CERTIFICATE PROFILE.....	73
7.1.1	<i>Base Certificate</i> .....	73
7.1.2	<i>Use of Extensions</i> .....	74
7.1.2.1	<i>Basic Constraints</i> .....	74
7.1.2.2	<i>Key Usage</i> .....	75
7.1.2.3	<i>Certificate Policies Extension</i> .....	75
7.1.2.4	<i>Authority Key Identifier</i> .....	75
7.1.2.5	<i>Subject Key Identifier</i> .....	75
7.1.2.6	<i>Subject Alternate Name</i> .....	75
7.1.2.7	<i>CRL Distribution Points</i> .....	76
7.1.3	<i>Algorithm Object Identifiers</i> .....	76

7.1.4	<i>Name Forms</i> .....	76
7.1.5	<i>Name Constraints</i> .....	76
7.1.6	<i>Certificate Policy Object Identifier</i> .....	76
7.1.7	<i>Usage of Policy Constraints</i> .....	76
7.1.8	<i>Policy Qualifiers Syntax and Semantics</i> .....	76
7.1.9	<i>Processing Semantics for the Critical Certificate Policy Extension</i> .....	76
7.2	CRL PROFILE .....	77
7.2.1	<i>Version numbers</i> .....	77
7.2.2	<i>CRL and CRL Entry Extensions</i> .....	77
<b>8</b>	<b>SPECIFICATION ADMINISTRATION</b> .....	<b>78</b>
8.1	SPECIFICATION CHANGE PROCEDURES .....	78
8.2	PUBLICATION AND NOTIFICATION PROCEDURES .....	78
8.3	CPS APPROVAL PROCEDURES .....	78
8.4	WAIVERS .....	78
	<b>APPENDIX A - DEFINITIONS</b> .....	<b>79</b>

# 1. INTRODUCTION

The Department of Defense has identified Public Key Infrastructure (PKI) as a critical underpinning of the Department's Information Assurance (IA) framework, and has established a roadmap for providing comprehensive PKI services to support all of the department's IA requirements. Within that framework, the DOD identifies the need to establish External Certification Authorities (ECA) to provide PKI services for non-DOD entities in a manner that is consistent with DOD security, functional, and interoperability requirements.

The DOD is in the process of finalizing the requirements for an ECA. Some programs, however, require immediate services of an ECA. To address these near-term requirements, and in an effort to provide the DOD and industry with initial experience with the ECA process, the DOD is planning to establish one or more Interim External Certification Authorities (IECA). It is expected that an approved DOD IECA will be authorized to provide PKI services for a period of 1 year or more until the final ECAs are operational.

This VeriSign DOD IECA Certification Practice Statement (CPS), in conjunction with the associated DOD IECA Memorandum of Agreement (MOA) and Minimum Requirements Document Version 1.3 (MR), presents the practices that VeriSign will employ in issuing and managing certificates and in maintaining a certificate-based public key infrastructure (PKI). It details and controls the certification process, from establishing IAs, commencing IA and repository operations, to enrolling subscribers. The VeriSign DOD IECA Certification Service provides for issuing, managing, using, suspending, and revoking non-DOD entity certificates.

The VeriSign DOD IECA has established a self-signed "trust anchor" (or Root CA) that will serve as the anchor of trust for all subscriber certificates issued by the VeriSign IECA. This VeriSign DOD IECA CPS is posted in the VeriSign repository at <http://www.verisign.com/gov/ieca/index.html>.

## **1.1 Overview**

This Certification Practice Statement is the statement of practices that VeriSign will employ when issuing certificates as an IECA. This CPS is structured in accordance with RFC 2527 of the Internet Engineering Task Force (IETF). The VeriSign DOD IECA service offering provides complete certificate life-cycle support and certificate repository services for approved non-DOD entities.

The architecture and functional solution for the VeriSign DOD IECA offering is based on VeriSign's commercial OnSite enterprise PKI solution. VeriSign has deployed one of the

industry's most robust and trusted PKI service offerings, and has undergone an independent audit of its security controls by KPMG. VeriSign's commercial customers in the banking, brokerage, financial, high tech, automotive, pharmaceutical, and many other vertical industries accept these security controls as the de facto industry standard.

The VeriSign DOD IECA primary location will be established at the VeriSign data center in Mt. View, CA. Authorized VeriSign personnel will perform the CA and RA functions. The RA, however, will rely on a delegated in-person identity proofing function performed by registered notaries public. Prior to issuing a DOD IECA end-entity certificate, the VeriSign RA must receive a notarized form from the subscriber that includes a statement of affiliation from the subscriber's affiliated company. The VeriSign RA will review the documents for integrity and consistency, and verify the legal existence of the company.

The end-entity certificate life cycle services for DOD IECA subscribers include:

- Registration: A subscriber must appear in person before a registered notary public, present a government-issued photo ID (passport, driver's license), and sign an acknowledgement letter. The notary witnesses these acts by affixing his or her seal/stamp on the certificate registration document. The subscriber mails the notarized registration form that includes a statement of affiliation from the subscriber's affiliated company to VeriSign via first class postal mail, Federal Express, or other similar means.
- Enrollment services: A subscriber will enroll for a certificate using a government-approved (FIPS 140-1 level 1) browser/platform configuration. Key generation is performed on the user's workstation within the FIPS-compliant browser, and the signed public key and identity information is sent securely (SSL 2) to the VeriSign DOD IECA.
- Enrollment verification: The subscriber's notarized enrollment form, including the affiliated company information, is checked for consistency with the subscriber's certificate enrollment request by the VeriSign DOD IECA RA. VeriSign will query the Dun & Bradstreet database to verify the existence of the company with which the subscriber is affiliated.
- Certificate issuance and distribution: Upon successful verification of the subscriber's enrollment request, the VeriSign DOD IECA will issue the certificate using a FIPS 140-1 level 2 hardware token. Once the subscriber's paper enrollment form is validated, the VeriSign DOD IECA RA will send e-mail to the subscriber with instructions on how to securely enroll and receive the certificate on-line.

- Certificate renewal: The current DOD IECA Minimum Requirements prohibit an IECA from renewing or updating IECA subscriber certificates. If the policy is amended to permit subscriber certificate renewal or updating, VeriSign will provide such a capability.
- Certificate revocation: Any DOD IECA subscriber will be able to revoke his or her certificate either by sending a digitally signed message to the VeriSign IECA, or automatically if the subscriber presents the unique challenge phrase selected by the subscriber during certificate enrollment to a revocation web page hosted by VeriSign. Upon successful validation of the revocation request, the certificate status in the database will be changed to revoked. Once every 24 hours, the VeriSign DOD IECA will prepare an updated certificate revocation list and post it to the repository.
- Certificate repository: Upon acceptance by the subscriber, VeriSign will publish all DOD IECA subscriber certificates to an LDAP-compliant directory. A subscriber will be given the option to remove his or her certificate entry from the repository. The VeriSign DOD IECA repository is accessible via an http query or via an LDAP-compliant client interface for relying parties to search and download DOD IECA subscriber certificates.
- System management functions (audit, archive, disaster recovery, etc.): The DOD IECA provides the requisite system management functions to ensure the availability and integrity of its data and services.

Approved DOD end-entities supported by the VeriSign DOD IECA are DOD contractors and vendors participating in specified programs requiring PKI support in the near-term. The VeriSign DOD IECA will issue DOD-compliant X.509 Version 3 certificates for use by DOD end-entities in a variety of secure commercial and government-developed applications such as electronic mail, signature of electronic forms and contract documents, secure document exchange, and secure web access and transmission.

Part of VeriSign's IECA offering is warranty protection under the NetSure<sup>SM</sup> Protection Plan. VeriSign will provide subscribers receiving certificates from the DOD IECA with limited warranties providing specified protection against compromise, impersonation, delay in properly communicating a request for revocation, unauthorized revocation, loss of use, or erroneous issuance. In addition, VeriSign will pay incidental and consequential damages sustained by these subscribers resulting from breaches of such warranties, up to certain limits. The certificates issued under this CPS are equivalent in assurance level to VeriSign Trust Network<sup>SM</sup> Class 3 certificates. Therefore, the provisions in the NetSure<sup>SM</sup> Protection Plan applying to Class 3 certificates apply to the certificates under

this CPS. In addition, the VeriSign DOD IECA shall be deemed an “issuing authority” within the meaning of the NetSure<sup>SM</sup> Protection Plan.

The limited warranties set forth within this CPS, but also appear in a separate NetSure<sup>SM</sup> Protection Plan document available in the VeriSign repository at <https://www.verisign.com/repository/netsure>. For further information, see the FAQ regarding the NetSure<sup>SM</sup> Protection Plan at [https://www.verisign.com/repository/netsure\\_faq](https://www.verisign.com/repository/netsure_faq).

## **1.2 Policy Identification**

This CPS describes VeriSign’s DOD IECA practices in support of the U.S. DOD IECA MOA and the Minimum Requirements Document Version 1.3.

The VeriSign DOD IECA will be operated as a dedicated PKI hierarchy with a single trust anchor. The established DOD IECA policy OID is as follows:

```
id-US-class 3::={joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101) dod(2)
infosec(1) certificate policy(11) 5}
```

## **1.3 Community and Applicability**

This CPS as well as the DOD X.509 CP describes a bounded public key infrastructure for non-DOD entities transacting electronic business with DOD entities. It describes the rights and obligations of persons and entities authorized under this Certification Practices Statement and Certificate Policy to fulfill any of the following roles: Certification Authority, Registration Authority, Notary, and Repository.

It also includes end-entity roles of Subscriber and Qualified Relying Party.

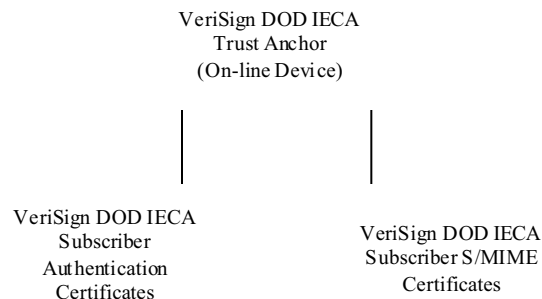
The Department of Defense dictates the applications suitable for DOD IECA certificates. Certificates will be used for, among other purposes, authenticated access to DOD systems that accept certificates. Current programs for which the DOD IECA is authorized to support include the Defense Travel System (DTS), Electronic Document Access (EDA), Wide Area Work Flow (WAWF), Medium Grade Services (MGS), and other applications or programs within the Department of Defense.

Digital Certificates issued under the DOD IECA are to be used solely for the purpose for non-DOD entities to transact electronic business with DOD entities. Any other use of DOD IECA Certificates is strictly prohibited.

### 1.3.1 CMI Authorities

#### 1.3.1.1 Certificate Authority (CA)

The VeriSign Certification Authority function of the DOD IECA will be operated at VeriSign’s primary CA facility in Mt. View, CA. The VeriSign DOD IECA will be a Certification Authority within a private hierarchy and serve as the “trust anchor” for certificates issued within the VeriSign DOD IECA domain. The VeriSign IECA will issue all end-entity certificates within the VeriSign DOD IECA domain. Figure 1 illustrates this hierarchy.



**Figure 1:** VeriSign DOD IECA Hierarchy

VeriSign will establish a single, self-signed (e.g. trust anchor) on-line Subscriber CA that will issue all IECA end-entity certificates. The VeriSign DOD IECA CA is responsible for the generation and management of non-DOD entity certificates and CRLs. These responsibilities include the processing of validated subscriber certificate requests and revocation requests, generation and sending of responses, generation of CRLs, posting of certificates and CRLs to the repository, designation of authorized RAs, and performing various system management and support functions.

All certificate signing key pairs will be 1024-bit RSA key pairs and will be generated, operated and controlled within VeriSign secure facilities using FIPS 140-1 Level 2 certified hardware devices.

#### 1.3.1.2 Registration Authority (RA)

VeriSign personnel will perform the RA function for the DOD IECA, co-located with the CA, within the VeriSign secure data facility located in Mt. View, CA. The RA relies on an in-person identity validation process performed by a notary public. The RA thereby delegates the authority to check the certificate applicant's forms of identification to the notary. The VeriSign IECA RA will not have a "pre-established" contractual relationship with the notary public community, but rather rely on the notary as State/Federal designated agents to perform a witness and acknowledgement function within the framework of widely accepted notary guidelines. The VeriSign RA who inspects the document for an official notary stamp or seal validates the authenticity of a notary "witnessed" document.

The VeriSign DOD IECA RA will be enrolled using an in-person registration process to issue a certificate, contained on a Smart Card, which provides secure authenticated access to the VeriSign DOD IECA. The RA is a VeriSign trusted person operating within VeriSign's secure facilities on VeriSign's internal corporate network.

#### 1.3.1.3 Repository

VeriSign will operate the DOD IECA Repository from its secure data facility located in Mt. View, CA. The LDAP-compliant directory contains DOD IECA end-entity certificates and CRLs. A DOD IECA subscriber may opt to have his or her certificate removed from this on-line repository.

Updates to the VeriSign DOD IECA Repository are controlled as only authorized processes and personnel may update repository records via simple (e.g. password) authentication. Subscribers and relying parties may query, view, and download certificate entries in the repository via a web interface or through an LDAP client.

### 1.3.2 Related Authorities

#### 1.3.2.1 Notaries

The VeriSign DOD IECA relies on the identity proofing services of State and Federal appointed notaries public. The notary public is responsible for validating the subscriber's identity using a government-issued photo ID and witnessing that the subscriber acknowledges his or her responsibilities and obligations as a DOD IECA subscriber and attests to the truth of the information in the certificate application. The

notary attests to these acts by signing the subscriber's enrollment form and applying his or her seal/stamp. For non-U.S. jurisdictions without notarial institutions, any requirement in this CPS for the use of a notary must be witnessed by an attorney, solicitor, embassy official, or other comparable authorized legal professional.

In addition to validating the identity of the subscriber, the notary validation process provides additional assurances against a false registration process. Having the subscriber acknowledge to the notary the validity and authenticity of the information on the subscriber enrollment form is a strong deterrent to falsification since such an act would constitute perjury in most notary jurisdictions.

### 1.3.2.2 Affiliated Company

The VeriSign DOD IECA will validate that the subscriber is affiliated with the company identified on the subscriber's enrollment form. The subscriber enrollment form has a section that must be signed by an authorized company representative (e.g. HR department) to attest to the subscriber's corporate affiliation, and to indicate company's approval for the named subscriber to use the resulting certificate to secure company transactions with the DOD. The VeriSign DOD IECA RA verifies the consistency between the name on the notarized enrollment form and the name on the subscriber's electronic certificate application. In addition, the VeriSign DOD IECA RA will query the Dun & Bradstreet database to verify the existence and legitimate name identified in the company employment letter.

### 1.3.2.3 Auditor

The VeriSign DOD IECA has identified a security manager who is responsible for the security and integrity of its operation. The security manager is a certified security specialist, who reports to the VeriSign Vice President of Practices and External Affairs. The Practices and External Affairs Department is organizationally separate from both the VeriSign engineering and operations departments.

VeriSign retains the services of an independent security audit firm, KPMG, which conducts a yearly examination of the controls associated with VeriSign's operations as set forth in VeriSign's practices documentation. The KPMG audit is performed in accordance with standards established by the American Institute of Certified Public Accounts (AICPA) as defined in the Statement of Auditing Standards (SAS) 70 and the WebTrust for CA guidelines. The most recent SAS 70 conducted by KPMG covered VeriSign commercial CA operations during the period of December 1 2000 to November 30 2001.

VeriSign is basing its DOD IECA CPS response on its existing commercial practices and controls. As such, the yearly independent SAS 70 and WebTrust for CA audits will provide the DOD assurance of VeriSign's compliance with the DOD IECA CPS.

#### 1.3.2.4 Policy Authority

The DOD PKI Steering Committee, a review committee composed of DISA and NSA personnel, constitutes the DOD IECA Policy Management Authority.

A DOD IECA operates under the auspices of a Memorandum of Agreement signed by the DOD Chief Information Officer.

### 1.3.3 End-Entities

#### 1.3.3.1 Subscribers

A DOD IECA subscriber is any non-DOD entity authorized by the DOD to transact electronic business with a DOD entity. Examples of authorized DOD IECA subscribers include government contractors and vendors.

The DOD IECA is not authorized to issue end-entity certificates for DOD entities.

#### 1.3.3.2 Relying Parties

A DOD IECA relying party is a DOD end-entity acting through an individual or application that accepts a secure transaction from a DOD IECA subscriber.

### 1.3.4 Applicability

Examples of suitable applications include, but are not limited to:

- (a) User authentication and access control to contract and financial documents;
- (b) User authentication and data integrity for forms associated with DOD contracts;  
and,
- (c) Secure electronic mail between DOD contractors and DOD entities.

Certificates issued under this CPS 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 communications systems, air traffic control systems, or weapons control systems, where failure could lead directly to death, personal injury, or severe environmental damage.

## **1.4 Contact Details**

### **1.4.1 Specification Administration Organization**

The VeriSign Controls Committee is responsible for maintaining and interpreting the DOD IECA CPS.

### **1.4.2 Contact Persons**

Parties having questions as to the content, applicability, or interpretation of this CPS may address their comments to either:

James Brandt  
Director Federal Markets  
VeriSign, Inc.  
1190 Winterson Road  
Linthicum, MD 21090  
410-691-2100  
federal@verisign.com

Anthony Miller

VeriSign, Inc.  
487 East Middlefield Road  
Mt. View, CA 94043  
650-429-3425  
practices@verisign.com

### **1.4.3 Person Determining CPS Suitability for the Policy**

The DOD Policy Management Authority determines the suitability of the VeriSign DOD IECA CPS and its compliance with the DOD CP.

## **2. GENERAL PROVISIONS**

This Section sets forth general provisions of obligations and defines and allocates specific responsibilities among the various parties participating in the trust network established by this CPS. These parties are:

- Certification Authority;
- Registration Authority;
- Subscriber
- Relying Party, and
- Repository

The parties are hereby notified of the following rules and obligations governing the respective rights and obligations of the parties among themselves. These rules and obligations are deemed to be agreed by the parties effective:

1. upon publication of this CPS in the case of the CA, RA, and Repository;
2. upon submission of an application for a certificate, in the case of a Subscriber; and
3. upon reliance of a certificate or digital signature verifiable with reference to a public key listed in the certificate, in the case of a Relying Party or other recipient of a certificate issued under this CPS.

Additional obligations are set forth in other provisions of this CPS, Relying Party Agreements, and the Subscriber Agreements.

### **2.1 Obligations**

#### **2.1.1 CA Obligations**

The VeriSign DOD IECA accepts the following obligations.

- VeriSign has submitted this CPS to the DOD IECA Policy Management Authority and it shall conform to this CPS and utilize trustworthy systems in performing its services.
- The VeriSign DOD IECA is obligated to all that reasonable rely on the information contained in the certificate that the certificate was issued to the named subscriber as witnessed by the notary, that the information in the certificate is accurate and

consistent with the identity information so witnessed by the notary (including, but not limited to the subscriber Distinguished Name in the subject field and the subject public key information field), and that the subscriber has accepted the certificate.

- The VeriSign DOD IECA is obligated to ensure that the subscriber who is the subject of the certificate is notified of the certificate issuance. Direct notification to the subscriber is accomplished through HTML form and e-mail processes. In addition, all DOD IECA subscriber certificates are published to the VeriSign DOD IECA repository.
- The VeriSign DOD IECA is obligated to ensure that the subscriber who is the subject of a certificate is notified of the certificate revocation. This notification is performed by including the certificate serial number of the revoked subscriber certificate on the Certificate Revocation List issued and maintained by the VeriSign DOD IECA and posted daily to the VeriSign DOD IECA Repository. The VeriSign DOD IECA is obligated to notify persons other than the subscriber of the revocation of such subscriber's certificate by the same means.
- The VeriSign DOD IECA is obligated to maintain records necessary to support requests concerning its operation, including audit files and archives.
- VeriSign shall protect the private key of the DOD IECA in accordance with CPS section 6.2.

### 2.1.2 RA Obligations

The VeriSign DOD IECA RA is obligated to accurately check the consistency of the information contained within enrollment forms submitted to VeriSign, as notarized by a notary public; to ensure that the enrollment form contains appropriate attestation of the subscriber's employment or affiliation with a company; to confirm the existence of that company; and to process requests and responses in a timely and secure manner. The RA shall conform to this CPS and utilize trustworthy systems in performing its services. The RA shall protect the RA private key in accordance with CPS section 6.2.

### 2.1.3 Subscriber Obligations

The following summarizes the obligations and responsibilities of a subscriber who has received a certificate from the VeriSign DOD IECA:

- Certificate applicants shall submit certificate applications and accept certificates in accordance with CPS sections 4.1, 4.3.
- Subscribers are obligated to provide accurate information required of them in a certificate application.

COPYRIGHT © 2000 VERISIGN, INC. ALL RIGHTS RESERVED.

- Subscribers are obligated to protect their private keys at all times, in accordance with section 6.2 this CPS and local procedure.
- Subscribers are obligated to notify the VeriSign DOD IECA immediately upon any suspected or actual compromise of their private keys.
- Subscribers are obligated to abide by all restrictions placed upon the use of their private keys and certificates.
- Users agree not to monitor, interfere with, or reverse engineer the technical implementation of the VeriSign DOD IECA except as explicitly permitted by this CPS or upon written approval by VeriSign.
- Certificate applicants and subscribers will not submit to VeriSign, an IA, or the VeriSign repository any materials that contain statements that (i) are libelous, defamatory, obscene, pornographic, abusive, bigoted, hateful, or racially offensive, (ii) advocate illegal activity or discuss illegal activities with the intent to commit them, or (iii) otherwise violate any law.

#### 2.1.4 Relying Party Obligations

The following summarizes the obligations and responsibilities of a relying party who has received a certificate from the VeriSign DOD IECA repository or by other means:

- Relying parties are obligated to use the certificate for the purpose for which it was issued. Users must independently assess and determine the appropriateness of certificates issued under this CPS for any particular purpose.
- Relying parties are obligated to establish trust in the VeriSign DOD IECA by developing or obtaining, and then verifying the certificate chain starting from a trust anchor of the relying party. The path processing shall comply with the guidelines set by the X.509 v3 Amendment.
- Relying parties are obligated to check each certificate in the certificate chain for revocation or suspension before its use.
- Relying parties are obligated to verify the digital signature of the VeriSign DOD IECA that issued the certificate they are about to use.

Relying parties that do not perform the obligations in this section assume all risks with regard to the digital signature and/or certificate on which they are relying.

## 2.1.5 Repository Obligations

The VeriSign DOD IECA Repository is obligated to provide certificates, CRLs and other revocation information, and other information as prescribed by VeriSign from time to time. The VeriSign repository is accessible at <https://www.verisign.com/gov/ieca> and by other communications methods as may be designated by VeriSign from time to time. VeriSign may publish both within and outside of the VeriSign repository a subscriber's certificate and CRL-related data. This CPS prohibits accessing of any data in the repository (or data otherwise maintained by an IA) that is declared confidential by the CPS and/or by the VeriSign repository, unless authorized by VeriSign.

Currently, the VeriSign DOD IECA Repository is implemented using the Netscape LDAP directory technology. The VeriSign DOD IECA Repository provides unrestricted access to subscribers, relying parties, and other interested parties through HTTP query and automated LDAP client interfaces.

## **2.2 Liability**

### 2.2.1 Warranties and Limitations on Warranties

#### 2.2.1.1 CA Warranties

This section sets forth the warranties made by VeriSign, the disclaimers of warranties of VeriSign, and limitations on VeriSign's liability. Subscribers and relying parties have warranty protection under the NetSure<sup>SM</sup> Protection Plan ("Plan") as described in CPS § 1.1 in connection with the applications described in CPS § 1.3. As mentioned in CPS § 1.1, the provisions in the Plan applying to Class 3 certificates apply to the certificates under this CPS, and the VeriSign DOD IECA shall be deemed an "issuing authority" within the meaning of the Plan. The protections VeriSign provides to subscribers and relying parties under the Plan are set forth in CPS § 2.2.1, disclaimers of warranty and liability under the Plan appear in CPS § 2.2.2, and the Plan's limitations of liability appear in CPS § 2.2.3.

Subscribers have additional protections under the Plan when relying on any VeriSign Certificates outside the context of the applications described in CPS § 1.3 and the certificates issued under this CPS. See the Plan at <http://www.verisign.com/netsure> for a full description of these protections. CPS § 2.2.1 is limited to subscribers' protections in connection with the applications described in CPS § 1.3, in which subscribers will not be relying upon certificates issued under this CPS.

#### 2.2.1.1.1 Scope of the NetSure<sup>SM</sup> Protection Plan

##### 2.2.1.1.1.1 *Who is Covered*

The Plan covers the following “covered persons”:

**(i) Subscribers.** Subscribers receiving certificates from the VeriSign DOD IECA are covered persons. To the extent a subscriber is an employee and is using his or her certificate on behalf of such employer, then such employer has the rights of such subscriber to the extent the employer sustains consequential or incidental damages resulting from a breach of one or more of the limited warranties in CPS § 2.2.1.1.2. Subscribers are entitled to the rights and protections under the Plan and CPS § 2.2.1 only if they are using their certificates for purposes and applications within the public key infrastructure in which non-DOD entities transact electronic business with DOD entities as described in CPS § 1.3. When they use or rely on certificates beyond those purposes or applications (e.g., personal use), they are considered to have the rights and protections only of relying parties, and not subscribers.

**(i) Relying Parties.** Relying parties are also covered persons under the Plan.

(a) A DOD end-entity that is not a natural person is capable of relying on a certificate. Such reliance can occur when an employee, agent, or application of such DOD end-entity relies on a certificate while acting on behalf of the DOD end-entity, regardless of whether such employee, agent, or application is a subscriber or the subject of a certificate.

(b) For purposes of the Plan, the relying party with respect to any certificate is the end-entity, on whose behalf its employee, agent, or application acts by relying on a certificate for the purpose of receiving or submitting any bid, offer, solicitation, purchase order, request for proposal (“RFP”), request for information (“RFI”), RFP or RFI response, or any other communication, or otherwise acts for the purpose of entering into any transaction. The relying party shall be the DOD entity having the capacity to contract that enters into such transaction or that is the intended sender or recipient of any such bid, offer, solicitation, purchase order, RFP, RFI, RFP or RFI response, or communication. For example, if a subscriber sends a digitally signed bid to each of six U.S. Army bases as part of these bases’ procurement of needed supplies, and each base relies on the subscriber’s certificate, each of the six bases is a relying party. All of the bases are relying parties even though they are within the organization of a single overarching entity, the Department of the Army, and ultimately the DOD.

#### *2.2.1.1.1.2 When the Coverage Applies*

Each type of covered person has a time period (“applicable time period”) in which the covered person’s limited warranty coverage under the Plan is in effect.

(a) **Subscribers.** For subscribers, the applicable time period is the operational period of their certificates.

(b) **Relying Parties.** For relying parties, the applicable time period is anytime, as long as the relying party is relying on a certificate to verify a digital signature made by the subscriber or for access control during the certificate's operational period, or to make an encrypted communication during such operational period.

#### 2.2.1.1.2 What is covered

(i) **Limited Warranty Regarding a Subscriber's Certificate.** VeriSign warrants to subscribers that at the time of issuance of his/her/its own certificate:

(a) there are no material misrepresentations of fact in such certificate known to VeriSign originating from VeriSign,

(b) there are no errors in the information in such certificate that were introduced by VeriSign as a result of its failure to exercise reasonable care in creating the certificate, and

(c) such certificate meets all material requirements of this CPS.

(ii) **Limited Warranty Regarding the Certificates of Others.** VeriSign warrants to all relying parties that rely, during the applicable time period, on a public key operation completed using the public key listed in a certificate issued under this CPS, that at the time such certificate is issued:

(a) all information in or incorporated by reference in such certificate, except non-verified subscriber information, is accurate, and

(b) VeriSign has substantially complied with this CPS when issuing such certificate.

(iii) **Limited Warranty Against Unauthorized Use, Unauthorized Disclosure, and Compromise.** VeriSign warrants that during the applicable time period the private key corresponding to the public key in the certificates listed in this Section below will not be subject to unauthorized use or disclosure prior to the revocation or expiration of such certificates. VeriSign makes this warranty:

(a) to subscribers, to the extent the warranty relates to their own certificates,

(b) to relying parties, to the extent the warranty relates to the valid operational certificates of others issued under this CPS on which a relying person relies.

This warranty includes, without limitation, the unauthorized use or disclosure of the private key of the VeriSign DOD IECA, and the unauthorized use or disclosure of a private key following a compromise of such private key.

This limited warranty shall not apply if the unauthorized use or disclosure is wholly or partially caused by a covered person's intentional conduct or failure to exercise reasonable care to safeguard his/her/its private key from unauthorized use or disclosure. For information regarding Private Key protection, *see* [https://www.verisign.com/repository/PrivateKey\\_FAQ/index.html](https://www.verisign.com/repository/PrivateKey_FAQ/index.html).

*Note:* When a Covered Person relies on the certificate of a subscriber by authenticating the public key in such certificate by validating a certificate chain, the covered person is also relying upon the certificates of the issuing authorities in the certificate chain.

**(iv) Limited Warranty Against Unauthorized Revocation and Loss of Use.**

VeriSign warrants that during the applicable time period the certificates listed in this Section below will be free from unauthorized revocation or loss of use caused by VeriSign. VeriSign makes this warranty:

(a) to subscribers, to the extent the warranty relates to their own operational certificates,

(b) to relying parties, to the extent the warranty relates to the valid operational certificates of others issued under this CPS on which a relying party relies.

**(v) Limited Warranties Against Erroneous Issuance and Impersonation.**

VeriSign warrants that during the applicable time period, the certificates listed in this Section below were issued to the persons named as the subjects of such certificates and were not issued as a result of erroneous issuance, including but not limited to erroneous issuance resulting from impersonation. VeriSign makes this warranty:

(a) to subscribers, to the extent the warranty relates to them and their own certificates,

(b) to relying parties, to the extent the warranty relates to the valid operational certificates of others issued under this CPS on which a relying party relies.

**(vi) Limited Warranty Regarding Delay in Requesting Revocation.**

VeriSign warrants to relying parties that during the applicable time period, the relying party will not be materially and adversely affected when relying on the valid certificates of subscribers as a result of such subscribers' reasonable delay in properly communicating a request for revocation of their certificates.

### 2.2.1.1.3 Payments and Payment Requests

**(i) NetSure Payments.** Subject to the limitations in CPS § 2.2.1.1.4, VeriSign shall pay a covered person for any incidental or consequential damages caused by a breach of one or more of the limited warranties in CPS § 2.2.1.1.2 made to the covered person.

**(ii) Requirements for Making a Payment Request.** As a condition to payment under CPS § 2.2.1.1.3(i), a covered person must (a) make a payment request by completing and submitting the payment request form at [https://www.verisign.com/repository/netsure\\_pay](https://www.verisign.com/repository/netsure_pay); (b) provide other information reasonably requested by VeriSign, its agents, or its employees (including without limitation proof of the covered person's damages); (c) provide reasonable cooperation with any investigation concerning damages to the covered person; (d) subrogate and assign to VeriSign any and all claims and causes of action such covered person has against third parties for damages or other relief that may potentially reimburse VeriSign for payments made by VeriSign to such covered person hereunder, up to the amount paid by VeriSign under CPS § 2.2.1.1.3(i).

**(iii) Notice.** Covered persons shall give VeriSign prompt notice of any breach(es) of the limited warranties in CPS § 2.2.1.1.2 in the manner set forth in CPS § 2.4.2.4 or CPS § 2.2.1.1.3(ii).

**(iv) Limitations Period.** VeriSign shall have no obligation to make a payment under CPS § 2.2.1.1.3(i) for a breach of one of the CPS § 2.2.1.1.2 warranties unless the covered person submits a payment request as required by CPS § 2.2.1.1.3(ii) for that payment within one (1) year after following:

(a) in the case of subscribers, the end of the operational period of their certificates; or

(b) in the case of relying parties, the breach of warranty.

#### 2.2.1.1.4 Limitations on Payments

**(i) \$1,000 Limitation on Payments to Relying Parties.** The most that VeriSign must pay a relying party for a single incident resulting in a breach of one or more of the CPS § 2.2.1.1.2 limited warranties made to the relying party is \$1,000. Notwithstanding the foregoing, if a single incident resulting in such a breach results in losses to multiple relying parties that are Affiliated Individuals as to a common entity, then the most that VeriSign must pay for that incident is \$1,000. "Affiliated Individual" shall mean a human being that is related to an 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. For example, if such a breach arose out of a digitally signed e-mail sent to two covered persons who are employees of the same company, then the most VeriSign would pay one or both employees is \$1,000. The limitations in CPS § 2.2.1.1.4(ii)-(iii) do not apply to Non-NetSure Relying Parties.

**(ii) Limitation on Payments to Subscribers.** The most that VeriSign must pay a subscriber under CPS § 2.2.1.1.3(i) is the “certificate lifetime limit” that applies under CPS § 2.2.1.1.4(iii).

**(iii) Certificate Lifetime Limit.** The certificate lifetime limit for certificates issued under this CPS is \$50,000.

**(a) How the Certificate Lifetime Limit Works.** The certificate lifetime limit is the most that VeriSign must pay a subscriber for any and all breaches of CPS § 2.2.1.1.2 limited warranties during the applicable time period or for breaches of the limited warranties under the Plan when relying upon certificates outside the context of the applications in CPS § 1.3. All payments under CPS § 2.2.1.1.3(i) or otherwise under the Plan for non-CPS applications reduce the amount of the certificate lifetime limit available for future payments. Once the certificate lifetime limit of a subscriber is exhausted by payments under CPS § 2.2.1.1.3(i) or otherwise under the Plan, VeriSign has no further obligation to make further payments under CPS § 2.2.1.1.3(i) or the Plan for breaches relating to that subscriber or his/her/its certificate. Nonetheless, when certificates are renewed at the end of their operational period, the new certificate issued upon renewal has its own new certificate lifetime limit.

**(b) Erroneous Issuance and/or Impersonation.** One kind of breach of CPS § 2.2.1.1.2(v) is erroneous issuance and/or impersonation resulting in the issuance of a VeriSign certificate incorrectly naming a subscriber. *Note:* The VeriSign certificate issued because of erroneous issuance is not the same as the subscriber’s own certificate issued under this CPS.

When this kind of breach occurs, only one certificate lifetime limit applies to the breach. In addition, the certificate lifetime limit applicable to the breach is the one for the subscriber’s own certificate, not the certificate lifetime limit of the VeriSign certificate resulting from erroneous issuance. If the subscriber has more than one certificate, then the subscriber can choose which of these certificates will provide the certificate lifetime limit for the breach. A covered person cannot choose a certificate to the extent that its certificate lifetime limit has already been exhausted. Any payments made under CPS § 2.2.1.1.3(i) or otherwise under the Plan reduce the applicable certificate lifetime limit.

The issuance of one VeriSign certificate as a result of erroneous issuance and/or impersonation is a single breach of CPS § 2.2.1.1.2(v) regardless of: how many relying parties rely on that VeriSign certificate, the amount or number of payments that a covered person may need to pay to satisfy claims asserted by these relying parties, or the number or amount of other losses sustained by the covered person as a result of the issuance of such VeriSign certificate, or the number of other certificates held by the covered person.

(iv) **Other Remedies.** The limitations on damages and payments in CPS § 2.2.1.1.4(ii)-(iii) do not apply to refund payments under CPS § 2.5.5 or general contract damages.

#### 2.2.1.1.5 Persons Excluded from Protections

**VERISIGN PROVIDES THE LIMITED WARRANTIES IN CPS § 2.2.1.1.2 ONLY TO THE COVERED PERSONS IDENTIFIED IN CPS § 2.2.1.1.1.1. VERISIGN MAKES NO WARRANTY UNDER THIS PLAN TO ANY OTHER PERSONS. THE PLAN AND THE OBLIGATIONS CONTAINED IN IT AND IN CPS § 2.2.1.1 ARE NOT FOR THE BENEFIT OF ANY PERSONS OTHER THAN COVERED PERSONS. THIS CPS IS NOT INTENDED TO CREATE ANY THIRD PARTY BENEFICIARY RIGHTS FOR ANY PERSON.**

#### 2.2.1.1.6 Exceptions to Limited Warranties

The limited warranties in CPS § 2.2.1.1.2 do not apply to losses or damages of a covered person, caused wholly or partially by:

(a) Reliance upon information contained in or incorporated in a certificate, whether or not published in the VeriSign repository, where such reliance is unreasonable or unjustified for any reason, in light of, among other things, facts that the covered person knows or should know, course of dealing between pertinent parties, or usage of trade.

(b) The failure or unreasonable delay of such covered person to properly communicate a request for revocation of a VeriSign certificate as required by the CPS.

(c) The failure of such covered person to exercise reasonable care to prevent compromise of the subscriber's own private key, failure to use a trustworthy system, or breach of any material obligation under the CPS or subscriber agreement.

(d) The failure of such covered person relying upon a subscriber's or an issuing authority's VeriSign certificate to apply reasonable security measures to verify the digital signature of such subscriber or such issuing authority. For a discussion of security measures used when verifying digital signatures or relying on certificates, *see* <https://www.verisign.com/repository/digidfaq.html>.

(e) The failure of such covered person to apply reasonable security measures prior to and during the creation, storage, and transfer of encrypted messages prepared for a subscriber of a certificate for purposes of sharing confidential or secret data with such subscriber as an intended recipient, including without limitation (i) the failure to determine that such subscriber's certificate is an operational certificate and (ii) the failure to validate a certificate chain for such subscriber's certificate.

(f) The failure of such covered person or of any subscriber to use an RSA Public Key algorithm with at least the designated and available modulus size.

(g) The failure of such covered person or of any subscriber to use any public key algorithm other than RSA.

(h) Any condition or incident of *force majeure* under the CPS or subscriber agreement.

(i) Acts by any person whose unauthorized conduct damages, alters, impedes, or otherwise misuses the facilities or services of Internet service providers or other providers of telecommunications or value-added services, including but not limited to the use or reproduction of malicious software such as computer viruses.

(j) The failure of communications infrastructure, processing, or storage media or mechanisms, including components thereof not under the exclusive ownership or control of VeriSign.

(k) Brown-outs, power failures, or other disturbances to electrical power.

(l) Illegal acts by the covered person, by a subscriber, or by any person relying on a certificate.

(m) Illegal acts by a person coercing the covered person to perform acts causing the covered person's loss or damages.

(n) Use or reliance upon demo, test, or free certificates.

(o) Such covered person's monitoring, interfering with, or reverse engineering, directly or indirectly, the technical implementation of the VeriSign Trust Network or other VeriSign certification services, unless expressly permitted by the CPS or upon prior written approval of VeriSign.

#### 2.2.1.2 RA Warranties

VeriSign performs both CA and RA functions. Accordingly, for a description of VeriSign's warranties, *see* CPS § 2.2.1.1.

#### 2.2.1.3 Subscribers' Representations

##### 2.2.1.3.1 General Representations

By accepting a certificate issued by VeriSign, the subscriber certifies to and agrees with VeriSign and to all who reasonably rely on the information contained in the certificate that

at the time of acceptance and throughout the operational period of the certificate, until notified otherwise by the subscriber,

(i) 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, suspended or revoked) at the time the digital signature is created,

(ii) no unauthorized person has ever had access to the subscriber's private key,

(iii) all representations made by the subscriber to VeriSign regarding the information contained in the certificate are true,

(iv) all information contained in the certificate is true to the extent that the subscriber had knowledge or notice of such information and does not promptly notify the IA of any material inaccuracies in such information as set forth in CPS § 4.3.1,

(v) the certificate is being used exclusively for authorized and legal purposes, consistent with this CPS, and

(vi) the subscriber is an end-user subscriber and not an IA, and will not use the private key corresponding to any public key listed in the certificate for purposes of signing any certificate (or any other format of certified public key) or CRL, as an IA or otherwise, unless expressly agreed in writing between subscriber and the IA.

**BY ACCEPTING A CERTIFICATE, THE SUBSCRIBER ACKNOWLEDGES THAT HE, SHE, OR IT AGREES TO THE TERMS AND CONDITIONS CONTAINED IN THIS CPS AND THE APPLICABLE SUBSCRIBER AGREEMENT.**

#### 2.2.1.3.2 Representations Relating to Intellectual Property Infringement

Certificate applicants (and, upon acceptance, subscribers) represent and warrant that their submission (to VeriSign) and use of a domain and distinguished name (and all other certificate application information) does not interfere with or infringe upon the rights of any third parties in any jurisdiction with respect to their trademarks, service marks, trade names, company names, or any other intellectual property right, and that they are not seeking to use the domain and distinguished names for any unlawful purpose, including, without limitation, tortious interference with contract or prospective business advantage, unfair competition, injuring the reputation of another, and confusing or misleading a person, whether natural or incorporated. Certificate applicants (and, upon acceptance, subscribers) shall defend, indemnify, and hold VeriSign harmless for any loss or damage resulting from any such interference or infringement.

## 2.2.2 Disclaimers of Warranty and Liability

### 2.2.2.1 SPECIFIC DISCLAIMERS

**EXCEPT AS EXPRESSLY STATED IN CPS § 2.2.1.1.2, ISSUING AUTHORITIES:**

**(A) DO NOT WARRANT THAT NONVERIFIED SUBSCRIBER INFORMATION CONTAINED IN VERISIGN CERTIFICATES IS ACCURATE, AUTHENTIC, RELIABLE, COMPLETE, CURRENT, MERCHANTABLE, OR FIT FOR A PARTICULAR PURPOSE,**

**(B) SHALL NOT INCUR LIABILITY TO ANY PERSON FOR REPRESENTATIONS CONTAINED IN A VERISIGN CERTIFICATE, PROVIDED THE CERTIFICATE WAS PREPARED SUBSTANTIALLY IN COMPLIANCE WITH THE CPS, AND PROVIDED FURTHER THAT THE FOREGOING DISCLAIMER SHALL NOT APPLY TO VERISIGN'S LIABILITY IN TORT FOR NEGLIGENT, RECKLESS, OR FRAUDULENT CONDUCT,**

**(C) DO NOT WARRANT "NONREPUDIATION" FOR ANY VERISIGN CERTIFICATE OR ANY MESSAGE (BECAUSE NONREPUDIATION IS DETERMINED EXCLUSIVELY BY LAW AND THE APPLICABLE FINAL DISPUTE RESOLUTION MECHANISM), AND**

**(D) DO NOT WARRANT THE STANDARDS OR PERFORMANCE OF ANY HARDWARE OR SOFTWARE NOT UNDER EXCLUSIVE OWNERSHIP OF, EXCLUSIVE CONTROL OF, OR LICENSED TO VERISIGN.**

***SEE ALSO* CPS § 2.3.2 (DISCLAIMER OF FIDUCIARY RELATIONSHIP).**

### 2.2.2.2 GENERAL DISCLAIMER

**EXCEPT AS EXPRESSLY PROVIDED IN CPS § 2.2.1.1.2 AND THE APPLICABLE SUBSCRIBER AGREEMENT, AND TO THE EXTENT PERMITTED BY APPLICABLE LAW, ISSUING AUTHORITIES DISCLAIM ANY AND ALL OTHER EXPRESS OR IMPLIED WARRANTIES AND OBLIGATIONS OF ANY TYPE TO ANY PERSON, INCLUDING ANY WARRANTY OF MERCHANTABILITY, ANY WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE, AND ANY WARRANTY OF THE ACCURACY OF INFORMATION PROVIDED BY CERTIFICATE APPLICANTS, SUBSCRIBERS, AND THIRD PARTIES, AND FURTHER DISCLAIM ANY AND ALL LIABILITY FOR ANY ACTS BY VERISIGN THAT CONSTITUTE OR MAY BE HELD TO CONSTITUTE STRICT LIABILITY, WHETHER SOLE OR JOINTLY WITH ANY OTHER PERSON, INCLUDING BUT NOT LIMITED TO ANY COVERED PERSON.**

## 2.2.3 Limitations of Liability

### 2.2.3.1 LIMITATIONS ON AMOUNT OF DAMAGES

**IN THE EVENT A SUBSCRIBER OR RELYING PARTY INITIATES ANY CLAIM, ACTION, SUIT, ARBITRATION, OR OTHER PROCEEDING SEPARATE FROM A REQUEST FOR PAYMENT UNDER SECTION CPS § 2.2.1.1.3(ii), AND TO THE EXTENT PERMITTED BY APPLICABLE LAW, VERISIGN'S LIABILITY SHALL BE LIMITED AS FOLLOWS:**

**(a) THE TOTAL LIABILITY OF VERISIGN IN TORT FOR NEGLIGENT, RECKLESS, OR FRAUDULENT CONDUCT IN CONNECTION WITH A SINGLE TRANSACTION SHALL BE LIMITED TO \$1,000,000 US. THE LIABILITY CAPS PROVIDED IN THIS SECTION SHALL BE THE SAME REGARDLESS OF THE NUMBER OF DIGITAL SIGNATURES, ACTS OF AUTHENTICATION, OR ENCRYPTED MESSAGES RELATED TO, OR CLAIMS ARISING OUT OF, SUCH TRANSACTION.**

**(b) SUBJECT TO THE FOREGOING SUBSECTION (a), THE TOTAL LIABILITY OF VERISIGN FOR GENERAL CONTRACT, TORT, OR ANY OTHER DAMAGES SUSTAINED BY ANY AND ALL SUBSCRIBERS AND RELYING PARTIES, COMBINED WITH ANY AND ALL DAMAGES SUSTAINED BY ANY AND ALL OTHER PERSONS CAUSED BY THE USE OF OR RELIANCE ON A SPECIFIC CERTIFICATE ISSUED UNDER THIS CPS ("NON-NETSURE DAMAGES") SHALL BE LIMITED TO AN AMOUNT NOT TO EXCEED \$100,000, FOR THE TOTAL OF ALL DIGITAL SIGNATURES, TRANSACTIONS, AND CLAIMS RELATED TO SUCH CERTIFICATE. THE LIABILITY CAPS PROVIDED IN THIS SUBSECTION SHALL BE THE SAME REGARDLESS OF THE NUMBER OF DIGITAL SIGNATURES, TRANSACTIONS, OR CLAIMS RELATED TO SUCH CERTIFICATE. IN THE EVENT THE NON-NETSURE DAMAGES SUSTAINED BY THE USE OR RELIANCE ON A SPECIFIC CERTIFICATE EXCEED THE LIABILITY CAP FOR SUCH CERTIFICATE, PAYMENT OF NON-NETSURE DAMAGES SHALL BE APPORTIONED FIRST TO THE EARLIEST CLAIMS TO ACHIEVE FINAL RESOLUTION (BY SETTLEMENT OR OTHERWISE), UNLESS OTHERWISE ORDERED BY A COURT OF COMPETENT JURISDICTION. SUBJECT TO SECTIONS 2.2.1.1.3 AND 2.5.5 OF THE CPS, VERISIGN SHALL NOT BE OBLIGATED TO PAY MORE THAN THE TOTAL LIABILITY CAP FOR EACH CERTIFICATE, REGARDLESS OF THE METHOD OF APPORTIONMENT AMONG CLAIMANTS OF THE AMOUNT OF THE LIABILITY CAP. THIS SECTION APPLIES TO LIABILITY UNDER CONTRACT (INCLUDING BREACH OF WARRANTY), TORT (INCLUDING STRICT LIABILITY), AND ANY OTHER LEGAL OR EQUITABLE FORM OF CLAIM.**

**(c) THIS SECTION 2.2.1.4.1 DOES NOT LIMIT REFUND PAYMENTS UNDER CPS § 2.5.5 OR PAYMENTS UNDER CPS § 2.2.1.1.3(i). THIS SECTION 2.2.1.4.1 APPLIES ONLY TO THE EXTENT PERMITTED BY APPLICABLE LAW.**

### **2.2.3.2 EXCLUSION OF CERTAIN ELEMENTS OF DAMAGES**

**EXCEPT AS EXPRESSLY PROVIDED IN CPS § 2.2.1.1.3, AND TO THE EXTENT PERMITTED BY APPLICABLE LAW, VERISIGN SHALL NOT BE LIABLE IN CONTRACT TO ANY PERSON FOR ANY INDIRECT, SPECIAL, RELIANCE, INCIDENTAL, OR CONSEQUENTIAL DAMAGES (INCLUDING BUT NOT LIMITED TO ANY LOSS OF PROFITS OR LOSS OF DATA), ARISING FROM OR IN CONNECTION WITH THE USE, DELIVERY, LICENSE, PERFORMANCE, OR NONPERFORMANCE OF CERTIFICATES, DIGITAL SIGNATURES, OR ANY OTHER TRANSACTIONS, PRODUCTS, OR SERVICES OFFERED OR CONTEMPLATED BY THIS CPS, EVEN IF VERISIGN HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.**

**TO THE EXTENT PERMITTED BY APPLICABLE LAW, VERISIGN SHALL NOT BE LIABLE TO ANY PERSON FOR ANY PUNITIVE DAMAGES ARISING FROM OR IN CONNECTION WITH THE USE, DELIVERY, LICENSE, PERFORMANCE, OR NONPERFORMANCE OF CERTIFICATES, DIGITAL SIGNATURES, OR ANY OTHER TRANSACTIONS OR SERVICES OFFERED OR CONTEMPLATED BY THIS CPS.**

## ***2.3 Financial Responsibility***

VeriSign has sufficient financial resources to maintain its operations and perform its duties, and it is reasonably able to bear the risk of liability to subscribers and recipients of certificates and other persons who may rely on the certificates and time stamps it issues. VeriSign also maintains \$50M of insurance coverage for errors and omissions.

### **2.3.1 Subscriber's Liability and Indemnity**

Without limiting other subscriber obligations stated in this CPS, subscribers are liable for any misrepresentations they make in certificates to third parties who, having verified one or more digital signatures with the certificate, reasonably rely on the representations contained therein.

**BY ACCEPTING A CERTIFICATE, THE SUBSCRIBER AGREES TO INDEMNIFY AND HOLD VERISIGN AND ITS AGENT(S) AND CONTRACTORS HARMLESS FROM ANY ACTS OR OMISSIONS RESULTING IN LIABILITY, ANY LOSS OR DAMAGE, AND ANY SUITS AND**

**EXPENSES OF ANY KIND, INCLUDING REASONABLE ATTORNEYS' FEES, THAT VERISIGN AND ITS AGENTS AND CONTRACTORS MAY INCUR, THAT ARE CAUSED BY THE USE OR PUBLICATION OF A CERTIFICATE, AND THAT ARISES FROM (i) FALSEHOOD OR MISREPRESENTATION OF FACT BY THE SUBSCRIBER (OR A PERSON ACTING UPON INSTRUCTIONS FROM ANYONE AUTHORIZED BY THE SUBSCRIBER); (ii) FAILURE BY THE SUBSCRIBER TO DISCLOSE A MATERIAL FACT, IF THE MISREPRESENTATION OR OMISSION WAS MADE NEGLIGENTLY OR WITH INTENT TO DECEIVE THE VERISIGN OR ANY PERSON RECEIVING OR RELYING ON THE CERTIFICATE; OR (iii) 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.**

### 2.3.2 Fiduciary Relationships

**VERISIGN IS NOT THE AGENT, FIDUCIARY, TRUSTEE, OR OTHER REPRESENTATIVE OF SUBSCRIBERS OR RELYING PARTIES.** The relationship between VeriSign and subscribers and that between VeriSign and relying parties is not that of agent and principal. Neither subscribers nor relying parties have any authority to bind VeriSign, by contract or otherwise, to any obligation. VeriSign shall make no representations to the contrary, either expressly, implicitly, by appearance, or otherwise.

### 2.3.3 Administrative Processes

An annual report of VeriSign can be obtained by submitting a written request to the address specified in section 1.4. The annual report discusses the financial auditing of VeriSign and the accounting standards underlying such auditing.

## ***2.4 Interpretation and Enforcement***

### 2.4.1 Interpretation

#### 2.4.1.1 Governing Law

If you are an individual or entity within the United States Government, this Agreement, and the interpretation of it, will be governed, as applicable, by the Contract Disputes Act of 1978, as amended (codified at 41 U.S.C. § 601 *et seq.*). For individuals or entities not within the United States Government, the laws of the state of California, U.S.A., shall govern the enforceability, construction, interpretation, and validity of this CPS, irrespective of contract or other choice of law provisions and without the requirement to establish a commercial nexus in California. This choice of law is made to ensure uniform

procedures and interpretation for all users, no matter where they reside or use their certificates.

#### 2.4.1.2 Conflict of Provisions

In the event of a conflict between this CPS and other rules, guidelines, or contracts, the subscriber shall be bound by the provisions of this CPS, except as to other contracts either (i) predating the first public release of the CPS or (ii) expressly superseding this CPS for which such contract shall govern as to the parties thereto, and except to the extent that the provisions of this CPS are prohibited by law.

#### 2.4.1.3 Interpretation

Unless otherwise provided, this CPS shall be interpreted consistently with what is commercially reasonable under the circumstances. In interpreting this CPS, regard is to the benefits in promoting uniformity in its application, and to the observance of good faith.

#### 2.4.1.4 Headings and Appendices of this CPS

The headings, subheadings, and other captions in this CPS are for convenience and reference only and shall not be used in interpreting, construing, or enforcing any of the provisions of this CPS. The appendices, including the definitions to this CPS, are for all purposes an integral and binding part of the CPS.

### 2.4.2 Severability, Survival, Merger, and Notice

#### 2.4.2.1 Severability

If any provision of this CPS, or the application thereof, is for any reason and to any extent found to be invalid or unenforceable, the remainder of this CPS (and the application of the invalid or unenforceable provision to other persons or circumstances) shall be interpreted so as best to reasonably effect the intent of its parties. **IT IS EXPRESSLY UNDERSTOOD AND AGREED THAT EACH AND EVERY PROVISION OF THIS CPS THAT PROVIDES FOR A LIMITATION OF LIABILITY, DISCLAIMER OF OR LIMITATION UPON ANY WARRANTIES OR OTHER OBLIGATIONS, OR EXCLUSION OF DAMAGES IS INTENDED TO BE SEVERABLE AND INDEPENDENT OF ANY OTHER PROVISION AND IS TO BE ENFORCED AS SUCH.**

#### 2.4.2.2 Survival

The obligations and restrictions contained within CPS §§ 2.7 (Audit), 2.8 (Confidential Information), CPS §§ 2.2.1.1.5-2.2.1.1.6, 2.2.2, 2.2.3 (Limitations on and Disclaimers of Warranty and Limitations of Liability), and CPS § 2.4 (Miscellaneous Provisions) shall survive the termination of this CPS.

#### 2.4.2.3 Merger

No term or provision of this CPS directly affecting the respective rights and obligations of VeriSign may be orally amended, waived, supplemented, modified, or terminated, except by an authenticated message or document of such affected party, except to the extent provided otherwise herein.

#### 2.4.2.4 Notice

Whenever any person hereto desires or is required to give any notice, demand, or request with respect to this CPS, such communication shall be made either using digitally signed messages consistent with the requirements of this CPS, or in writing. Electronic communications shall be effective upon the sender's receiving a valid, digitally signed acknowledgment of receipt from the recipient. Such acknowledgment must be received within five (5) days, or else written notice must then be communicated. Communications in writing must be delivered by a courier service that confirms delivery in writing or via certified or registered mail, postage prepaid, return receipt requested, addressed as follows:

To VeriSign:	VeriSign, Inc. 487 East Middlefield Road Mountain View, CA 94043 USA Attn: Certification Services (+1 650-961-8820)
By VeriSign	To the most recent address of record
to another person:	on file with VeriSign, Inc.

## 2.4.3 Dispute Resolution Procedures and Choice of Forum

### 2.4.3.1 Notification Among Parties to a Dispute

Before invoking any dispute resolution mechanism (including litigation or arbitration, as detailed below) with respect to a dispute involving any aspect of this CPS or a certificate issued by VeriSign under this CPS, aggrieved persons shall notify VeriSign and any other party to a dispute for the purpose of seeking dispute resolution among themselves.

### 2.4.3.2 Formal Dispute Resolution

If you are an individual or entity within the United States Government, this CPS, and the interpretation of it, will be governed, as applicable, by the Contract Disputes Act of 1978, as amended (codified at 41 U.S.C. § 601 *et seq.*). For individuals or entities not within the United States Government, and if negotiations do not resolve the dispute, an aggrieved person may invoke a dispute resolution mechanism as follows. Nothing in CPS § 2.4.3.2 shall preclude VeriSign from seeking equitable (including injunctive) relief upon alleged compromise or alleged material breach in a manner consistent with governing law and this CPS. Disputes involving federal government entities shall be resolved in accordance with applicable federal law. Otherwise, disputes shall be resolved in accordance with CPS § 2.4.3.2(i)-(ii).

**(i) When each indispensable party to a dispute is a Canadian or U.S. resident or organization situated or doing business in Canada or the United States.** Except where each indispensable party to a dispute agrees to an alternative dispute resolution mechanism (such as arbitration), all suits to enforce any provision of this CPS or arising in connection with the CPS or any related business relationship between the parties hereto shall be brought in the United States District Court for the Northern District of California or the Superior or Municipal Court in and for the County of Santa Clara, California, U.S.A. Each person hereby agrees that such courts shall have exclusive in personam jurisdiction and venue with respect to such person and each person hereby submits to the exclusive in personam jurisdiction and venue of such courts. The parties hereby waive any right to a jury trial regarding any action brought in connection with this CPS or the VeriSign Trust Network. Where an alternative dispute resolution is chosen by the parties, California law shall govern arbitability and procedure.

**(ii) Where one or more parties to a dispute is not a Canadian or U.S. resident or organization situated or doing business in Canada or the United States.** All disputes arising in connection with the CPS shall be finally settled under the Rules of Conciliation and Arbitration of the International Chamber of Commerce (ICC) modified as necessary to reflect the provisions herein by one or more arbitrators. The place of arbitration shall be in New York or San Francisco, U.S.A., and the proceedings shall be conducted in English. In cases involving a single arbiter, that single arbiter shall be

appointed by mutual agreement of the parties. If the parties fail to agree on an arbiter within fifteen (15) days, the ICC shall choose an arbiter knowledgeable in computer software law, information security, and cryptography or otherwise having special qualifications in the field, such as a lawyer, academician, or judge in a common law jurisdiction.

#### 2.4.4 Successors and Assigns

This CPS inures to the benefit of, and shall be binding upon the successors, executors, heirs, representatives, administrators, and assigns, whether express, implied, or apparent, of the parties. The rights and obligations detailed in this CPS are assignable by the parties, by operation of law (including as a result of merger or a transfer of a controlling interest in voting securities) or otherwise, provided such assignment is undertaken consistent with CPS § 4.9, concerning termination or cessation of CA operations; and provided further, that such assignment does not effect a novation of any other debts or obligations the assigning party owes to other parties at the time of such assignment.

#### 2.4.5 No Waiver

Failure by any person to enforce a provision of this CPS will not be deemed a waiver of future enforcement of that or any other provision.

#### 2.4.6 Compliance with Export Laws and Regulations

Export of certain software used in conjunction with the VeriSign Trust Network may require the approval of appropriate government authorities. The parties shall conform to applicable export laws and regulations.

#### 2.4.7 Choice of Cryptographic Methods

All persons acknowledge that they (not VeriSign) are solely responsible for and have exercised independent judgment in choosing security software, hardware, and encryption/digital signature algorithms, including their respective parameters, procedures, and techniques.

#### 2.4.8 Force Majeure

VeriSign shall not be responsible for any breach of warranty, delay, or failure in performance under this CPS that results from events beyond its control, such as acts of God, acts of war, epidemics, power outages, fire, earthquakes, and other disasters.

## **2.5 Fees**

### **2.5.1 Certificate Issuance or Renewal Fees**

The VeriSign DOD IECA will publish its fees for a subscriber certificate on its web site at <https://www.verisign.com/gov/ieca>. Such fees are subject to change seven (7) days following their posting in the VeriSign DOD IECA Repository.

### **2.5.2 Certificate Access Fees**

No stipulation.

### **2.5.3 Revocation or Status Information Access Fees**

No stipulation.

### **2.5.4 Fees for Other Services**

No stipulation.

### **2.5.5 Refund Policy**

The VeriSign DOD IECA adheres to, and stands behind, rigorous practices and policies in undertaking certification operations and in issuing certificates. Nevertheless, if for any reason a subscriber is not completely satisfied with the certificate issued to him, her, or it, the subscriber may request the VeriSign revoke the certificate within thirty (30) days of issuance and provide the subscriber with a refund. Following the initial thirty (30) day period, a subscriber may request that VeriSign revoke the certificate and provide a refund if VeriSign has breached a warranty or other material obligation under this CPS or the NetSure Protection Plan relating to the subscriber or the subscriber's certificate. After VeriSign revokes the subscriber's certificate, VeriSign will promptly credit the subscriber's credit card account for the full amount of the applicable fees paid for the certificate. To request a refund, subscribers shall complete the Refund Request Form at <https://www.verisign.com/repository/refund>. This refund policy is not an exclusive remedy and does not limit other remedies that may be available to subscribers.

## **2.6 Publication and Repositories**

### **2.6.1 Publication of CA Information**

The VeriSign DOD IECA will operate an online Repository available to Subscribers and Relying Parties. This Repository will contain or provide access to the following minimum information:

1. all valid and un-expired VeriSign DOD IECA Certificates;
2. certificate status information, including revocation;
3. certificate revocation lists that it issues;
4. the VeriSign DOD IECA certificate(s) needed to validate the signature on VeriSign DOD IECA subscriber certificates;
5. any other relevant information the VeriSign considers relevant regarding to the use of VeriSign DOD IECA certificates by its subscribers or relying parties.

The VeriSign DOD IECA CPS is considered VeriSign Proprietary information.

### 2.6.2 Frequency of Publication

All information to be published in the repository shall be published promptly after such information is available to the VeriSign DOD IECA.

Upon the subscriber's acceptance of the certificate, the VeriSign DOD IECA shall immediately publish a copy of the certificate in the VeriSign DOD IECA Repository.

Upon suspending or revoking a certificate, the VeriSign DOD IECA shall immediately publish notice of the revocation in the VeriSign DOD IECA Repository. A CRL will be created and published on a daily basis.

### 2.6.3 Access Controls

The VeriSign DOD IECA shall not impose any access restrictions to information published in its repository. Subscribers and relying parties may access certificate and CRL information via HTTP and LDAP queries.

Updates to information contained in the VeriSign DOD IECA repository shall be controlled via simple (password) authentication and limited to trusted VeriSign DOD IECA personnel.

### 2.6.4 Repositories

The VeriSign DOD IECA Repository is implemented using Netscape LDAP technology. End users may search using the LDAP protocol for end-user certificates by configuring their LDAP clients to use [directory.verisign.com](http://directory.verisign.com).

## **2.7 Compliance Audit**

### **2.7.1 Frequency of Compliance Audit**

Although there is no requirement for an IECA to obtain an initial compliance audit, the VeriSign DOD IECA will be operating in accordance with practices and controls consistent with its commercial PKI operation. VeriSign retains the services of a professional security-auditing firm, specializing in PKI security controls, to audit its commercial PKI operations on an annual basis.

The most recent security audit of VeriSign's commercial PKI operations performed covered VeriSign's commercial operations during the periods of December 1 2000 through November 30 2001. A copy of the auditor's report may be provided on a non-disclosure basis.

### **2.7.2 Identity/Qualifications of Reviewer**

The VeriSign DOD IECA auditor is KPMG, the same professional auditing firm responsible for conducting VeriSign's commercial PKI audit. KPMG is intimately familiar with VeriSign's practices and policies, as it has been performing these services for VeriSign for nearly five years. The KPMG auditing team has extensive experience in all relevant matters of physical, personnel, technical, COMSEC, COMPUSEC, and logical security. Specifically, the compliance audit team has the following applicable experience:

- a minimum of 5 years experience performing security audits;
- a minimum of 3 year PKI engineering/design experience;
- a minimum of 6 years cryptography engineering experience; and
- a minimum of 6 years computer security experience.

### **2.7.3 Auditor's Relationship to Audited Party**

KPMG is under a contractual relationship to VeriSign for its security audit services and has no responsibility for the conduct of the VeriSign DOD IECA operation.

### **2.7.4 Topics Covered by Audit**

The security audit inspects VeriSign's conformance to all functions material to the trustworthiness of the VeriSign DOD IECA.

The audit and inspection will be conducted pursuant to the guidance provided in the American Institute of Certified Public Accountants' (AICPA's) Statement on Auditing

Standards (SAS) Number 70, *Reports on the Processing of Transactions by Service Organizations*, Type Two Review.

### 2.7.5 Actions Taken as a Result of Deficiency

Any discrepancies between the VeriSign DOD IECA operation and the stipulations in this CPS will be immediately brought to the attention of the DOD PMA.

Corrective action regarding any deficiencies identified in the reviews will be undertaken in accordance with provisions governing such action and so agreed to by VeriSign and the DOD PMA.

### 2.7.6 Communication of Results

VeriSign shall publish a synopsis of the compliance audit, including notification of any material discrepancies found, on the VeriSign DOD IECA Repository. VeriSign will provide a copy of the inspection audit report, in whole, to the PMA.

## **2.8 Confidentiality**

### 2.8.1 Types of Information to Be Kept Confidential

The following information shall be considered received and generated in confidence by the VeriSign DOD IECA and may not be disclosed except as provided below:

- CA application records,
- Subscriber agreements and certificate application records (except for information placed in the VeriSign DOD IECA repository or certificate per this CPS),
- Transactional records (both full records and the audit trail of transactions),
- Audit trail records created or retained by VeriSign,
- Any private signature key within the VeriSign DOD IECA hierarchy,
- Contingency planning and disaster recovery plans, and
- Security measures controlling the operations of CA hardware and software and the administration of certificate services and designated enrollment services.

All confidential information shall be handled as sensitive, and access shall be restricted to those with official needs.

VeriSign shall not release or be required to release any confidential information without an authenticated, reasonably specific request prior to such release from (i) the person to whom VeriSign owes a duty to keep such information confidential and (ii) the person requesting confidential information (if not the same person); or court order.

The VeriSign DOD IECA shall not disclose or sell applicant names or other identifying information, and shall not share such information, except in accordance with this CPS.

### 2.8.2 Types of Information Not Considered Confidential

None of the information contained in the VeriSign DOD IECA repository or in subscriber certificates shall be considered confidential.

### 2.8.3 Disclosure of Certificate Revocation/Suspension Information

The fact that a particular subscriber certificate is revoked is not confidential; however, the transactional records and other information leading up to such a revocation is considered confidential information.

### 2.8.4 Release to Law Enforcement Officials

The VeriSign DOD IECA may release sensitive information based on a court-authorized order that is duly signed by a competent judge of a court, in the course of a criminal investigation.

### 2.8.5 Release as Part of Civil Discovery

No stipulation at this time.

### 2.8.6 Disclosure upon Owner's Request

See 2.8.4.

### 2.8.7 Other Information Release Circumstances

No stipulation at this time.

## **2.9 Intellectual Property Rights**

Unless otherwise agreed, property interests in the following security-related information materials and data are regarded as the property of the parties indicated below:

- Certificates: Certificates are the personal property of the VeriSign DOD IECA.

- CPS: This CPS is personal property of VeriSign, Inc.
- Distinguished Names: Distinguished names are the personal property of the persons named (or their employer or principal).
- Subscriber Private Keys: Subscriber private keys are the personal property of the subscribers who rightfully use or are capable of using them (or their employer or principal), regardless of the physical medium within which they are stored or protected.
- Subscriber Public Keys: Subscriber public keys are the personal property of subscribers (or their employers or principal), regardless of the physical medium within which they are stored or protected.
- VeriSign Private Keys: VeriSign DOD IECA private keys are the personal property of VeriSign, Inc.
- VeriSign Public Keys: VeriSign DOD IECA public keys are the property of VeriSign Inc. VeriSign licenses relying parties to use such keys.

## **3. IDENTIFICATION AND AUTHENTICATION**

### ***3.1 Initial Registration***

#### **3.1.1 Types of Names**

All certificates issued by the VeriSign DOD IECA shall use the DN name format for subject and issuer name fields. Refer to section 7.1.1 for the Name Form definition.

#### **3.1.2 Need for Names to be Meaningful**

Subscriber certificates issued by the VeriSign DOD IECA will contain the legal name of the person to whom the certificate is issued and the company name to which the subscriber is affiliated.

#### **3.1.3 Rules for Interpreting Various Name Forms**

See section 7.1.1.

#### **3.1.4 Uniqueness of Names**

The VeriSign DOD IECA will ensure the uniqueness of names for all certificates issued within the DOD IECA domain. The VeriSign DOD IECA shall create the common name component of the DN by appending a unique identifier (UID) to a name supplied by the subscriber during registration. Unique identifiers will be integers selected from a block of integers supplied by the DOD. The UID will be the same for all certificates (digital signature/non-repudiation and key encipherment) issued to a single subscriber.

#### **3.1.5 Name Claim Dispute Procedure**

The naming authority used by the VeriSign DOD IECA shall have sole discretion regarding the assignment of relative distinguished names and certificate serial numbers appearing in the certificates they issue.

#### **3.1.6 Recognition, authentication, and role of trademarks**

See CPS section 2.2.1.3.2.

### 3.1.7 Method to prove possession of private key

The VeriSign DOD IECA shall require proof that the subscriber has a functioning key pair. One technical mechanism to establish this proof is that the subscriber's enrollment request containing their public key is digitally signed with the corresponding private key. VeriSign will perform the digital signature validation checks to ensure this is a properly formed message and that its integrity has not been altered. Authentication of organization identity

The VeriSign DOD IECA shall validate the legal existence of the subscriber's employer and the affiliation of the subscriber with their employer. Specifically, the VeriSign DOD IECA RA will ensure the company's name is registered in the Dun & Bradstreet database and registered to do business under that name. Also, the subscriber must obtain a signed attestation (as provided on the subscriber enrollment form) from an appropriate company representative that validates his or her employment or other affiliation with that company.

### 3.1.8 Authentication of individual identity

Subscribers are required to appear in person to a notary to validate their identity prior to obtaining a certificate from the VeriSign DOD IECA. The subscriber must present a government-issued photo identity, such as a passport or driver's license, to the notary for this purpose.

The notary will also witness that the subscriber signs a Subscriber Enrollment Acknowledgement Letter that attests to his or her understanding of and agreement with his or her responsibilities as a subscriber, and that the information contained in the enrollment form is accurate. A copy of this signed SEAL is retained by the VeriSign DOD IECA.

## **3.2 Certificate Renewal, Update, and Routine Re-key**

### 3.2.1 Certificate re-key

By DOD policy, an IECA is not authorized to re-key, renew, or update a subscriber's certificate. If the policy is amended to permit subscriber certificate renewal or updating, VeriSign will provide such a capability.

The DOD IECA CA certificate will have a three- (3) year certificate validity period. Subscriber certificates issued by the VeriSign DOD IECA will have a one- (1) year validity period.

### 3.2.2 Certificate renewal

No stipulation.

### 3.2.3 Certificate update

No stipulation.

## **3.3 *Re-key After Revocation***

Subscribers must repeat the initial registration requirements, including in-person identity verification, for re-key after revocation.

## **3.4 *Revocation Request***

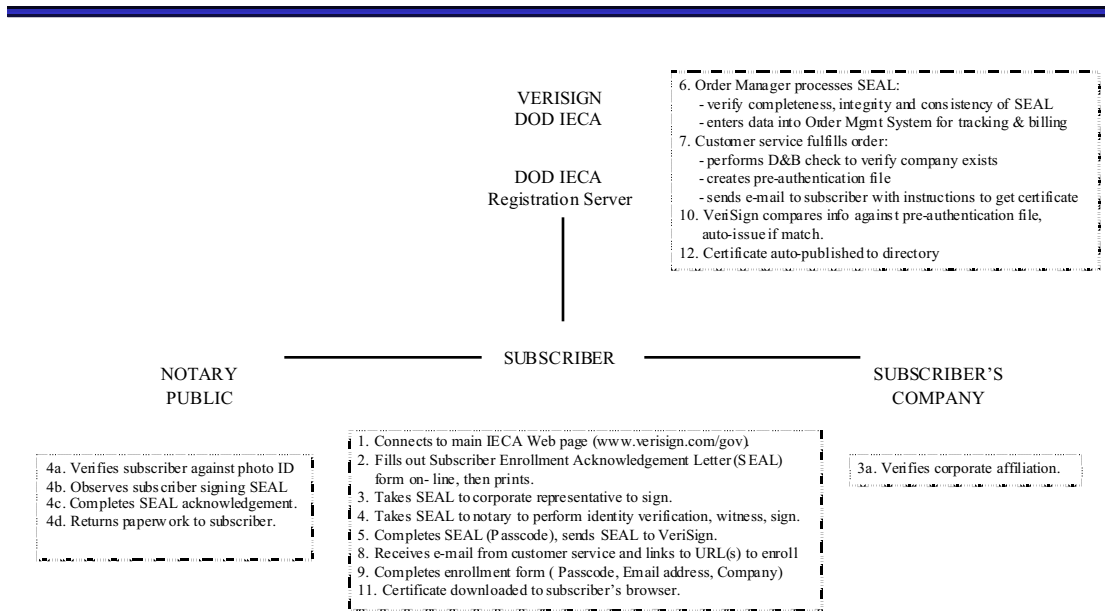
The VeriSign DOD IECA shall authenticate all requests for revocation. Only the subscriber may revoke his or her certificate by sending a digitally signed e-mail message to VeriSign or by presenting his or her challenge phrase selected during the certificate enrollment process.

The VeriSign DOD IECA RA may revoke a subscriber's certificate for cause.

## 4 OPERATIONAL REQUIREMENTS

Figure 4.1 describes the overall process for a subscriber to obtain a certificate from the

### VeriSign DOD IECA Enrollment Flow



VeriSign DOD IECA.

Figure 4.1 VeriSign DOD IECA Subscriber Enrollment & Authentication Process

#### 4.1 Certificate Application

Applicants first connect to a web page to obtain general instructions for how to prepare for and complete the certificate enrollment process. Additional information through FAQs, hyperlinks, etc., will also be available to assist applicants in understanding and using certificate technology.

Each applicant will complete a certificate application form (Subscriber Enrollment Acknowledgement Letter) on-line. The applicant prints the SEAL locally after completion on-line. The applicant must have an authorized company representative sign

Part I Section B of the SEAL. The applicant takes a government-issued photo identity (passport, driver's license), the SEAL, and notary payment (if any) to a notary public.

The notary public verifies the applicant's identity against the photo ID and verifies consistency with the applicant's identity on the SEAL. The applicant signs the SEAL acknowledging his or her understanding of subscribers' responsibilities and attesting to the accuracy of the information provided on the SEAL.

The notary signs the form, witnessing the applicant's signature and attestations, and affixes the notary's sign/seal. The notary (optionally) retains copies of the paperwork and then returns it to the subscriber, who mails the SEAL and employment verification letter to VeriSign.

#### **4.2 Certificate Issuance**

Upon receipt of the applicant's paperwork (SEAL and copy of photo ID shown to the notary for ID proofing), the VeriSign DOD IECA customer support specialist reviews the information for consistency and accuracy, and inspects the SEAL to ensure it has been properly notarized. The specialist queries the Dun & Bradstreet database, using the DUNS number supplied on the enrollment form, to validate the company's name and legal status.

If all checks pass, the VeriSign DOD IECA RA will send the subscriber an e-mail containing the URL where the subscriber must connect to enroll for his or her certificate. If the information entered on-line matches that provided to VeriSign on the SEAL, then the certificate will be automatically issued and returned immediately to the subscriber for local storage within the subscriber's browser.

Once the subscriber has accepted the certificate, it is posted into the VeriSign DOD IECA Repository.

#### **4.3 Certificate Acceptance**

A subscriber accepts a certificate once he or she enters the relevant enrollment information on-line and submits it to VeriSign for processing. The subscriber has the responsibility to contact the VeriSign DOD IECA to re-transmit the certificate in the event of a faulty download.

## **4.4 Certificate Suspension and Revocation**

### 4.4.1 Revocation

#### 4.4.1.1 Circumstances for Revocation

Under the following circumstances a certificate will be revoked:

- identifying information or attributes in the user certificate changes before the certificate expires;
- the certificate subject can be shown to have violated the stipulations of this CPS;
- the private key is suspected of compromise;
- the user or other authorized party asks for his/her certificate to be revoked.

Whenever any of the above circumstances occur, the associated certificate is revoked and placed on the CRL. Certificates remain on the CRL until they expire; they are removed from the second CRL issued after they expire.

#### 4.4.1.2 Who Can Request Revocation

The VeriSign DOD IECA RA can request the revocation of a subscriber's certificate on the subscriber's behalf, the subscriber's authorizing organization, or other authorized party. The subscriber is authorized to request the revocation of his or her own certificate.

#### 4.4.1.3 Procedure for Revocation Request

A subscriber or other authorized party may request revocation of the subscriber's certificate using any format that identifies the certificate to be revoked, explains the reason for revocation, and allows the request to be authenticated (e.g., digitally or manually signed). If the revocation is being requested for reason of key compromise or suspected fraudulent use, then the subscriber's and the RA's revocation request must so indicate.

A subscriber may revoke his or her own certificate by sending a digitally signed message to the VeriSign DOD IECA whereby the VeriSign DOD IECA RA will act upon the subscriber's request after first verifying the validity of the digitally signed message. Alternatively, if the subscriber is not in possession of their private signature key, he or she may also revoke his or her certificate by connecting to an HTML page to request such action. The subscriber must provide the correct challenge phase (selected by the subscriber during certificate enrollment) to authenticate himself or herself prior to VeriSign taking action on such a request.

Upon receipt and validation of a properly authenticated subscriber's request for certificate revocation, the VeriSign DOD IECA will immediately change the subscriber's certificate status to "revoked". Once a day, the VeriSign DOD IECA will aggregate all revoked certificates, digitally sign a new Certificate Revocation List, and post the CRL to the repository.

#### 4.4.1.4 Revocation Request Grace Period

The subscriber is obligated to request that the DOD IECA revoke his or her certificate as soon as possible after the need for revocation has been determined.

#### 4.4.2 Suspension

No stipulation.

#### 4.4.3 Certificate Revocation Lists

##### 4.4.3.1 CRL Issuance Frequency

The VeriSign DOD IECA will issue CRLs on a daily basis with a 1-week validity interval.

##### 4.4.3.2 CRL Checking Requirements

Relying parties are obligated to check for a new CRL daily.

#### 4.4.4 Online Status Checking

No stipulation.

#### 4.4.5 Other Forms of Revocation Advertisements Available

The VeriSign DOD IECA will also provide a Web-based query mechanism whereby relying parties may interactively inquire as to the revocation state of a VeriSign DOD IECA certificate.

#### 4.4.6 Special Requirements Related to Key Compromise

No stipulation.

## **4.5 Security Audit Procedures**

### **4.5.1 Types of Events Recorded**

VeriSign DOD IECA equipment will record events related to the server installation, modification, accesses and application requests, responses, actions, publications, and error conditions. The information recorded includes the type of event and the time the event occurred. Depending on the type of event, additional information such as the success or failure, the source and destination of a message or the disposition of a created object (e.g., a filename) will also be recorded. Electronic-based audit data is automatically collected. Physical data is recorded in a logbook, paper form, or other physical mechanism as appropriate to the process being audited.

Records are also maintained regarding modifications to the CA equipment configuration (e.g., changes in configuration files, security profiles, administrator privileges).

Logs used to record operator (for manned installations), room entry/exit, or security checks (per section 5.1.2) are kept for audit. Attempts to access the CA equipment, such as login to accounts or enabling cryptographic modules, are recorded. The records include the identity asserted in the attempt, the time, and the success or failure.

Requests, responses, and publications are recorded for audit review purposes. These include certificate creation, modification, and revocation requests and responses; certificate publication, receipt acknowledgment, and proof-of-possession messaging; key compromise notices and responses; and CRL and CPS publications.

Actions performed in carrying out requests and in support of normal operation of the CA equipment are recorded, such as certificate and CRL creation, accesses to CA databases, and use of the CA's signature key.

VeriSign records all audit events and record data (in either manual or electronic logs) specified in the IECA Minimum Requirements document. Specific audit events recorded include:

Events related to IECA (CA and RA) software:

- Installation: comply via the VeriSign change management process.
- Software modification: comply via the VeriSign change management process.
- Configuration modification: comply via the VeriSign change management process.
- Operator Login and Logouts:

- CA system operator role: event logged, group account (~ 10 individuals), individual I&A not currently performed
- DBA role: event logged, group account (2 individuals), individual I&A not currently performed
- Network Administrator: event logged, group account (~5 individuals), individual I&A not currently performed
- Firewall application: event logged, group account (~5 individuals), individual I&A not currently performed
- RA role: event logged, individual I&A maintained

Through the use of procedural and personnel controls, the VeriSign DOD IECA supports a system level I&A requirement.

Events related to IECA CA processing:

- Certificate generation requests: event recorded
- Certificate revocation requests: event recorded
- IECA responses: event recorded
- User confirmation: event recorded
- IECA actions: event recorded
- IECA publications: event recorded
- IECA re-key: event recorded
- Error conditions: event recorded

Events related to ID Proofing and RA processing:

- Authentication of user identity: notary responsible for retaining copy of method of ID proofing; VeriSign RA retains the SEAL and photo ID records submitted by subscribers.
- Certificate generation requests: event recorded.
- Certificate revocation requests: event recorded.
- IECA responses: event recorded.

COPYRIGHT © 2000 VERISIGN, INC. ALL RIGHTS RESERVED.

- Manual interactions with end-entities: significant events recorded.
- Interactions with IECA: events recorded.

#### 4.5.2 Frequency of Processing Log

The VeriSign DOD IECA implements a comprehensive system approach to actively detect erroneous operation of the system and to detect evidence of penetration attempts. The IECA certificate issuance and management application is designed to detect and record events that pertain to faulty or potentially insecure operation. The priority events that are logged to the error file are then examined by trusted operational personnel on a continuous basis. In addition, the IECA application performs a series of periodic self-tests to verify critical system operation. Failure of these self-tests will result in a page to operations personnel to take remedial action.

The DOD IECA system is designed to protect itself from unauthorized access by remote users to back-end functions or data. A number of intrusion prevention and detection mechanisms are configured to primarily prevent and then capture and report on certain events that may indicate unauthorized penetration attempts. The network operations personnel review these security logs at least weekly. Certain critical alerts will result in an immediate page of operational personnel.

#### 4.5.3 Retention Period of Audit Log

The DOD IECA has the ability to recover audit log information from on-line and archive storage. VeriSign currently retains all audit data of database records online to facilitate rapid response to audit-related issues. Audit logs are included in daily incremental and weekly full backups to facilitate recovery of the online system. Once a month, the full backup media is sent to a secure off-site facility for long-term (minimum of seven years) archive storage. Deletion of the audit log from the CA equipment is performed by an entity other than the authorized operators of our certification and validation services. The responsible individual is:

- John Ferguson  
Director of Production Services  
(650) 429-3350  
jferguson@verisign.com

Audit logs are retained as archive records in accordance with section 4.6.2 of this CPS.

#### 4.5.4 Protection of Audit Log

As a general design practice, the system audit log is not open for reading or modification by any human, or by any automated process other than those that perform audit

processing. Entities that do not have modification access to the audit log may archive it. Weekly/monthly audit data is moved to a safe, secure storage location separate from the CA equipment. The VeriSign DOD IECA current relies on procedural (personnel and facility) controls to protect audit records from accidental or malicious overwrite.

#### 4.5.5 Audit Log backup Procedures

The audit log is backed up on the same schedule as the rest of the data on the CA equipment. Incremental backups are produced daily. Full system backups are produced weekly.

#### 4.5.6 Audit Collection System

VeriSign produces audit data at the application, network and operating system level. Failure of the application level audit system is equivalent to cessation of operations inasmuch as the CA operations software is comprised in part of automated application audit functions

Audit processes are invoked at system startup, and only cease at system shutdown.

If it becomes apparent that an automated audit system has failed, CA operations cease until the audit capability is restored.

#### 4.5.7 Notification to Event-Causing Subject

No stipulation.

#### 4.5.8 Vulnerability Assessments

VeriSign has instituted a multi-faceted, proactive approach to ensuring a trustworthy IECA operation.

All personnel are trained as to their responsibilities and duties with regard to secure and trustworthy conduct. Managers and supervisors provide the first level of oversight, and the VeriSign Manager of Security provides an additional oversight and enforcement role.

Custom application software, combined with commercial off-the-shelf network and operation system level monitors, provide automated collection and some critical automated reporting capability. The priority events that are logged to the error file are examined by trusted operational personnel on a continuous basis.

VeriSign conducts quarterly vulnerability assessments to determine its ability to protect against external network threats. VeriSign personnel, in addition to external consultants, perform this routine assessment. Finally, VeriSign undergoes a yearly extensive SAS 70

Type 2-security audit to validate its operation in accordance with this practice documentation.

## **4.6 Records Archival**

### **4.6.1 Types of Data Archived**

The VeriSign IECA audit process records the following information, in either paper or electronic record format, upon initialization of a CA key pair:

- CA system equipment configuration files,
- CA accreditation (if necessary),
- Certification Practice Statement, and
- any contractual agreements to which the CA is bound.

The following data shall be recorded for archive during CA operation:

- modifications or updates to any of the above data items;
- all certificates and CRLs (or other revocation information) as issued or published;
- IECA public keys;
- weekly audit logs (in accordance with section 4.5);
- other data or applications sufficient to verify archive contents.

### **4.6.2 Retention Period for Archive**

VeriSign IECA archive records, including certificates, CRLs and IECA public keys, are retained for a period of at least 7 years. Currently, all database records are retained online for immediate access. Offsite storage of full systems backups is maintained to ensure recovery of the online system in the event of a catastrophic system fault.

### **4.6.3 Protection of Archive**

The ability to write to, modify, or delete the archive is strictly controlled. The contents of the archive are not released as a whole, except as required by law. Records of individual transactions may be released upon request of any entities involved in the transaction or their legally-recognized agents.

Archive media are only handled by trusted employees and stored in a separate, safe, secure storage facility on magnetic media. Archive records are labeled with the CA's distinguished name and the date of archive.

#### 4.6.4 Archive Backup Procedures

A full image tape backup of the VeriSign DOD IECA system and database is prepared once a week and sent to a secure off-site storage under the control of trusted personnel. Once a month, these full image backups are sent to a secure off-site location where they are retained for a minimum of 7 years.

#### 4.6.5 Archive Collection System

The VeriSign IECA (RA operator) will provide a copy of all certificates and CRLs issued during each 30-day period to the office designated by the DOD, upon request, within 10 days after a 30-day period has expired. Magnetic media, paper forms, or telephone dialogue will be used to transfer this information.

#### 4.6.6 Procedures to Obtain and Verify Archive Information

In the event it becomes necessary for an external party to obtain archive information, VeriSign Production Services personnel, upon receipt of a duly authorized request, will produce such information. This information will be produced from the current online data store (see Section 4.5.6) and written to magnetic media, which will be provided manually to a duly authorized agent of the external party requesting such information.

### **4.7 Key Changeover**

The DOD IECA will use its private signature keys for signing certificates and CRLs only. CA key pairs established under this CPS will be prevented by technical means from signing subscriber certificates whose validity periods would extend beyond the expiration dates of the CA certificate's validity interval.

CA certificate validity periods will be set to 3 years to ensure that the validity interval of user certificates, set to 1 year, will expire before the validity interval of the CA certificate. The DOD IECA will change its keys every 3 years, corresponding to the CA key validity period interval. The old IECA CA keys will be retained to issue CRLs for subscribers that have been issued certificates signed with the old IECA CA signing key.

## **4.8 Compromise and Disaster Recovery**

### **4.8.1 Compromise recovery**

In the event that the IECA key is compromised, the superior CA will list the serial number of the IECA's certificate on its CRL.

The VeriSign IECA will notify the DOD PKI Root CA and the DOD of a disaster or compromise via a commercially acceptable means of secure communication. DOD in turn will assist in communicating the revocation of the IECA certificate to all relying parties.

Subsequently, the VeriSign DOD IECA will reconstitute its operation under a new PKI hierarchy using the same procedures that were performed during initial system initialization and re-key all subscriber certificates.

### **4.8.2 Disaster Recovery**

In the case of a disaster in which the primary operational set of the VeriSign IECA equipment is damaged and inoperative, but the primary operational copy of the VeriSign IECA private key is not destroyed, the VeriSign IECA operations will be re-established as quickly as possible, giving priority to the ability to revoke subscribers' certificates. If the VeriSign IECA cannot reestablish revocation capabilities within the time periods specified in section 4.4.3, the VeriSign IECA will report its keys as compromised, and reestablish the CA keys and certificates, all cross-certificates, and finally all subscriber certificates.

In the case of a disaster whereby the VeriSign IECA installation is physically damaged and all copies of the primary operational copy of the VeriSign IECA signature key are destroyed as a result, the VeriSign IECA will initiate certificate management operations from its Disaster Recovery site.

#### **4.8.2.1 Disaster Recovery Process Initialization**

In the event of a natural or man-made disaster requiring temporary or permanent cessation of operations from VeriSign's primary facility, the VeriSign disaster recovery process is initiated by the VeriSign Emergency Response Team (VERT). This team consists of highly trusted VeriSign employees that have undergone extensive background checks, who will be deployed to perform an immediate assessment of the disaster situation and work with the Production Support, Certificate Signing Unit, and Customer Support teams. The planned target for recovery time is no more than 24 hours or better. The VERT consists of personnel from the following functional areas:

- Facilities

- Security
- Information Services
- Risk Management
- Finance
- Marketing
- Human Resources

This team immediately surveys the affected facilities and infrastructure, then makes a determination as to whether or not to declare a disaster. Members of this team are notified by the team leader/Business Resumption Manager that a catastrophic event has taken place and the team is mobilized. Once a disaster is declared, the Business Resumption Manager notifies our Disaster Recovery Facility and VeriSign begins restoration of its production capabilities within 24 hours.

There are six East Coast VeriSign employees on this team. Access to the physical infrastructure requires multiple members from the CSU Team. This team is trained in expeditiously activating the hardware/software for the CSUs.

#### 4.8.2.2 VeriSign Disaster Recovery Infrastructure

VeriSign maintains a Disaster Recovery Facility (DRF) located at a VeriSign-owned facility in Virginia. The VeriSign DRF is operated under similar security policies and procedures as the primary facility.

#### 4.8.2.3 Disaster Recovery At Time of Disaster (Hotsite)

In the event of a disaster, VeriSign will reconstitute its IECA operations at the DRF within 24 hours of the declared emergency.

### **4.9 CA Termination**

In the event that the VeriSign IECA is terminated for the convenience of the DOD, contract expiration, re-organization, or other non-security related reason, certificates issued by the VeriSign IECA will continue to be considered valid at the discretion of the program or relying party.

Upon direction of the DOD PMA, VeriSign will revoke the DOD IECA certificate and/or all subscriber certificates and destroy all IECA private keys. Dissemination of revocation notice will be achieved as discussed in CPS section 4.8.1.

The IECA shall transfer its archival records to the PMA, in a format specified in its CPS.

## **5 PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS**

### **5.1 Physical Controls**

#### **5.1.1 Site Location and Construction**

The system components and operation of the VeriSign DOD IECA will be contained within a physically protected environment to deter, detect, and prevent unauthorized use of, access to, or disclosure of sensitive information. The primary site location is at VeriSign headquarters in Mt View, CA., and the DRF is at a VeriSign-owned facility in Virginia. The facilities housing the primary and back-up CA and Repository provide extensive physical security and access control systems to limit access only to authorized personnel and authorized visitors. The physical security standards are designed and implemented consistent with the Department of Army Regulation 380-5, Information Security Program Guidance for the Classified Document and Material Storage Standards and Information.

The building's perimeter doors are of metal clad construction and doorframes are of appropriate strength. Locks are of appropriate construction and strength and building keys are controlled and managed. Perimeter walls are slab to slab in construction and there are no windows that open.

Security guards perform site parameter inspections once per hour.

#### **5.1.2 Physical Access**

The system components and operation of the VeriSign DOD IECA will be contained within a physically protected environment to deter, detect, and prevent unauthorized use of, access to, or disclosure of sensitive information.

The building has an alarm system that is actively monitored with redundant power and notification methods. Sensitive areas within the facility, such as power and network connection areas, are also controlled areas within the protected facility. The building's alarm system covering general work areas is activated at a minimum when the building is unattended for periods greater than 8 hours. However, at this point the VeriSign operations facility is manned around the clock. More sensitive areas of the facility, such as the data center containing active cryptographic modules are continuously alarmed and monitored.

The building has four Tiers of perimeter security enforced through employee ID badges, electronic keys (proximity cards), and biometric readers. Employees are required to wear a picture ID badge, and visitors are escorted at all times. All visitors must sign the visitor log (name, signature, company/organization, date/time, and escort) prior to obtaining a visitor badge.

The facility is continually staffed (24x7), either by trusted employees or by an on-site guard service. Background checks are performed on the guards who are specifically trained for the facility. Any change in guard personnel requires prior approval by the facilities or security manager. The guard force performs security checks at least once per 24 hours. A log will be retained describing the checks performed, the time, and the person who performed them. Specific checks made (either by the guard force or by designated trusted VeriSign DOD IECA personnel) for physical tampering will ensure that:

- IECA equipment, including cryptographic hardware and database disk arrays, is in a state appropriate for the current mode of operation;
- All security containers, including those containing cryptographic modules, and activation data, are properly secured;
- Physical security systems are functioning properly; and
- The building perimeter is secured against unauthorized access.

The building's access control system is continuously (24x7) armed. Guard personnel located in a security station monitor access to the building electronically and by video cameras. Access to Tiers 1 and 2 are controlled by electronic key. Electronic keys and biometric readers control access to Tiers 3 and 4. The access control system has an anti-passback feature that automatically arms itself when someone enters. It logs all entries, exits, and system events. There are redundant connections for remote monitoring, with wireless backup. The system's power is backed-up with battery and diesel generator. Video cameras provide 24 hour recording of access to the building, the roof, sensitive areas such as the data center, and the cryptographic key storage room.

Cryptographic hardware is stored in government approved safes requiring at least two trusted persons to access the material. Activation information is stored in locked containers separate from the cryptographic hardware.

### 5.1.3 Power and Air Conditioning

The VeriSign DOD IECA primary and backup facilities are supplied with power and air conditioning sufficient to create a reliable operating environment.

Power for the primary site is backed up in case of emergency failure. Should a major power failure occur, a battery based UPS system supplies sufficient power until the diesel generators are activated. The diesel generators are supplied from external to the building for unlimited refueling capacity.

#### 5.1.4 Water Exposure

No stipulation.

#### 5.1.5 Fire Prevention and Protection

An automated fire detection and suppression system has been installed in both the primary and backup facilities in accordance with local fire policy and code.

#### 5.1.6 Media Storage

Critical system data is incrementally backed-up on a daily basis. Full back-ups are performed on a weekly basis and the magnetic media is sent off site. The VeriSign DOD IECA has a disaster recovery (hot) site on the East Coast. Access to media is limited to authorized personnel and stored in fire-rated media safes.

#### 5.1.7 Waste Disposal

The VeriSign DOD IECA has disposal units for sensitive information separate from routine. Sensitive information is carefully handled prior to destruction in approved shredder machines.

#### 5.1.8 Off-Site Backup

See section 5.1.6.

### **5.2 Procedural Controls**

#### 5.2.1 Trusted Roles

The VeriSign DOD IECA and Repository will be operated in accordance with approved policy, practices, and procedures regarding safe and trustworthy system operation.

All employees, contractors, and consultants of the VeriSign DOD IECA and RA (collectively, "personnel") that have access to or control cryptographic operations that may materially affect the issuance, use, suspension, or revocation of certificates, including access to restricted operations of the Repository, are considered as serving in a trusted position. Such personnel include, but are not limited to, customer service personnel,

system administration personnel, security auditors, designated engineering personnel, and executives who are designated to oversee the trustworthy infrastructures.

Specifically, all employees whose duties include any of the following must acquire and periodically re-qualify (every five years) for “trusted employee” status as a condition of employment:

1. access to CSU devices or key shares;
2. access to production systems;
3. ability or authorization to issue certificates and CRLs;
4. holders of combinations to safes and/or keys to safety deposit boxes;
5. certificate authentication specialists;
6. certificate verification specialists;
7. personnel who have access to company or customer sensitive material;
8. company management (Director and above);
9. granters of physical and/or logical access;
10. security and auditing personnel;
11. ability or authorization to issue, renew, revoke, or replace certificates;
12. personnel who have access to company or customer sensitive material; or
13. granters of physical and/or logical access to customer information.

Within the context of the above trusted functions, the VeriSign DOD IECA operation manifests itself in a number of functional roles required to securely and efficiently operate and manage a large data center operation. The security-relevant roles are described as follows.

The *IECA CA System Operator* is responsible for successful initialization and subsequent operation of the CA application. IECA application processes have automated most of the operational functions normally identified with a CA operator (in the context of a CA workstation). These automated functions include: certificate generation and revocation; posting certificates and CRLs; certificate re-key, etc. Multiple trusted individuals perform this function through three operational shifts.

The *IECA DBA* is responsible for the successful initialization and subsequent healthy operation of the IECA database. Multiple trusted individuals perform this function.

The *IECA Network Administrator* is responsible to ensure the integrity and reliability of IECA internal and external communications and network level resources.

The *IECA Firewall Application Manager* is responsible for successful installation and subsequent management of the IECA firewalls to ensure appropriate protection from external threats.

The *IECA RA operator* is responsible for validating subscriber certificate enrollment requests. The RA will receive SEAL and employment verification information from a subscriber and will perform validation functions to ensure the SEAL was properly completed and notarized. The RA will assist subscribers during the enrollment process (as required), and will prepare routine media transfer of IECA certificates and CRLs to a designated government entity.

The *IECA Security Auditor* reports to the VeriSign Manager of Security, who is in a department separate from both engineering and operations. The IECA security auditor is responsible for overseeing daily security of IECA operations and compliance with this CPS, and does not perform any IECA operational role (CA/RA operator, DBA, etc.).

The *IECA Cryptographic Device Manager* is responsible for secure initialization and life cycle management of the IECA PKI hierarchy, including cryptographic module and activation data (key shares) initialization, storage, backup, and recovery.

In general, individuals assigned to one of these operational roles are not permitted to perform other trusted roles.

### 5.2.2 Number of Persons Required Per Task

The VeriSign DOD IECA maintains a policy and rigorous control procedures to ensure segregation of duties based on job responsibilities. The most sensitive tasks, such as access to and management of Cryptographic Signing Units (CSU) and associated key material, require multiple trusted employees.

These internal control procedures are designed to ensure that at a minimum, two trusted personnel are required to have either physical or logical access to the device. No employee is granted access to successive barriers (either physical or logical) to a CSU. Access to CSU cryptographic hardware is strictly enforced by multiple trusted employees throughout its lifecycle, from incoming receipt and inspection to final logical and/or physical destruction. Once a CSU is activated with operational keys, further access

controls are invoked to maintain split control over both physical and logical access to the device. Persons with physical access to CSUs do not hold key “shares,” and vice versa.

Upon cryptographic initialization of a CSU, logical access to the keyed device is controlled through multiple key shares. In general, 5 key shares are created and individually assigned to trusted employees. A minimum of 3 or the 5 shareholders must be present to activate a CSU.

### **5.3 Personnel Security Controls**

#### **5.3.1 Background, Qualifications, Experience and Clearance Requirements**

All persons with unattended access to the VeriSign DOD IECA and Repository are expressly approved and must be of unquestionable loyalty, trustworthiness, and integrity.

The VeriSign DOD IECA institutes an extensive personnel security program that identifies specific “high risk” duties and requires “trusted personnel” to be assigned to these duties. The trusted status is only granted upon successful completion of a background investigation, performed by an independent investigation firm. Employees are trained and made fully aware of their responsibilities to maintain compliance with corporate security, unique program security, and personal security/integrity requirements as a condition of continued employment as a trusted employee.

The scope of the background investigation is similar to the DOD Industrial Top Secret (TS) criteria. The only differences are how far back information is checked (seven years, as opposed to fifteen years), and the limitation that corporate checks cannot include certain Privacy Section questions included in the DOD TS investigation. VeriSign retains the services of an independent investigation firm to perform the background investigations on its current and potential employees. In the conduct of its background investigations, investigators perform the following checks:

1. criminal history (7-10 years);
2. credit history;
3. previous employment;
4. professional references;
5. education (verification of highest or most relevant degree);
6. DMV records; and

## 7. Social Security trace.

Information revealed during a background investigation that would preclude an employee or potential employee from obtaining “trusted employee” status includes, but may not be limited to the following:

1. any conviction or multiple arrests for a crime involving violence or attempted violence;
2. any conviction or multiple arrests for a crime involving theft or attempted theft;
3. any conviction or multiple arrests for a crime, other than mere possession of marijuana, involving controlled substances or illegal drugs;
4. any pattern of behavior indicating personal irresponsibility, such as:
  - (a) multiple driving under the influence arrests (lifetime);
  - (b) multiple declarations of bankruptcy (lifetime);
  - (c) multiple recent (5 years) credit problems, including missed mortgage or car payments;
  - (d) any embellishment on a resume or job application involving:
    1. falsely stating an employer or
    2. falsely stating academic qualifications.

### 5.3.2 Background Check Procedures

See section 5.3.1.

### 5.3.3 Training Requirements

Operations personnel are sufficiently trained prior to performing independent, unattended duties. The employee training program is typically 4-8 weeks in duration, consisting of: mentoring by a functional area expert and/or supervisor; video, Computer Based Training (CBT), and hands-on training; and formal testing and certification. Training topics include the operation of the IECA software and hardware, operational and security procedures, and stipulations of the ECA guidelines and the IECA CPS. Re-training is performed, as required, as new system functionality is deployed, or if there is any substantive change in DOD IECA security or operational procedures.

A training log is retained of each student who successfully completes a training (or re-training) module indicating the student trained, the training received, and the date the training was completed. The student is issued a certificate recognizing training successfully completed.

#### 5.3.4 Retraining Frequency and Requirements

See section 5.3.3.

#### 5.3.5 Job Rotation Frequency and Sequence

No stipulation.

#### 5.3.6 Sanctions for Unauthorized Actions

VeriSign DOD IECA personnel understand that service in the capacity of a trusted position is contingent on successful performance of the security and functional responsibilities commensurate with the trusted position.

#### 5.3.7 Contracting Personnel Requirements

Any VeriSign DOD IECA subcontractor employed for a position is held to the same functional and security criteria as if he or she were a full-time VeriSign employee.

#### 5.3.8 Documentation Supplied to Personnel

Documentation sufficient to define duties and procedures for a role shall be provided to the personnel filling that role.

## **6 TECHNICAL SECURITY CONTROLS**

### **6.1 Key Pair Generation and Installation**

#### **6.1.1 Key Pair Generation**

Key pairs are generated in such a way that the private key is not known by anyone other than the authorized user of the key pair. Subscriber key pairs are generated on the subscriber's local system. VeriSign DOD IECA key pairs are generated within VeriSign's secure Key Ceremony room on hardware tokens. At no time does the VeriSign DOD IECA appear in plain-text form outside the hardware protection boundary of the VeriSign DOD IECA hardware token.

#### **6.1.2 Private Key Delivery to Entity**

Private key delivery is accomplished by generating subscriber key pairs directly at the subscriber's local system. Transfer of subscriber keys and certificates within the subscriber's local environment is recommended using the protected PKCS#12 enveloping technique.

#### **6.1.3 Public Key Delivery to certificate issuer**

Subscriber public key delivery to the VeriSign DOD IECA will use the PKCS#10 construction. This mechanism ensures that:

1. the public key has not been changed during transit, and
2. the sender possess the private key corresponding to the transferred public key.

#### **6.1.4 CA Public Key Delivery to Users**

The VeriSign DOD IECA CA public key certificate will be posted at <https://www.verisign.com/gov/ieca>.

#### **6.1.5 Key Sizes**

All certificate signing key pairs and subscriber key pairs will be 1024-bit RSA key pairs.

#### **6.1.6 Public Key Parameters**

No stipulation for RSA.

### 6.1.7 Parameter quality checking

No stipulation for RSA.

### 6.1.8 Hardware/software key generation

Pseudo-random numbers used for CA key material are generated within a FIPS 140-1 level 2 hardware cryptographic module.

Key material used by the VeriSign DOD IECA RA is contained on a Smart Card.

See CPS section 6.2.1.

### 6.1.9 Key usage purposes

The VeriSign DOD IECA shall always include the key usage extensions and will mark that extension as critical.

See CPS section 7.1.

## **6.2 CA Private Key Protection**

### 6.2.1 Standards for cryptographic modules

VeriSign DOD IECA subscribers are obligated to use cryptographic modules that meet FIPS 140-1 Level 1 criteria, in accordance with the DOD CP and MR. The VeriSign DOD IECA uses FIPS 140-1 Level 2 certified hardware cryptographic tokens. VeriSign's key management facility, practices and procedures—audited by KPMG in our SAS/70 report—provide FIPS 140-1 Level 3 key management assurances.

All cryptographic modules dedicated to management of VeriSign DOD IECA certificate signing key pairs are operated such that the private asymmetric cryptographic keys are never output in plain-text.

The DOD IECA RA key and certificates are contained on industry-standard Smart Cards. The RA function is co-located with the IECA function and is performed by trusted IECA personnel located within the VeriSign DOD IECA trusted facility, which affords adequate protection to the RA key/certificate.

### 6.2.2 Private key multi-person control

Both the operational and backup versions of the VeriSign DOD IECA private key are subject to multi-person control over activation of the hardware token containing the

private key. A list identifying the parties responsible for this control will be made available for inspection during compliance audits.

When the VeriSign DOD IECA certificate signing key pair is generated in VeriSign's Key Ceremony facility, the PIN required to activate the associated hardware token is also generated automatically and is composed of a large random value. This value is automatically decomposed into multiple shares in an m-of-n secret sharing scheme. These shares are written to magnetic media and distributed individually to trusted employees (see Section 6.4 Activation Data for additional detail).

Once the token is so initialized, the key pair generated and the associated CA certificate signed by its superior CA, the token is ultimately moved to a separate Secure Data Center room for activation into an operational state. Activation of the token requires the personal presence of a designated quorum of shareholders established during the Key Ceremony. Each shareholder presents his or her value to the system intended to activate and use the token. After a quorum of such values is collected, this system automatically reconstitutes the PIN value and supplies this value in a software interface to the token for its activation.

### 6.2.3 Private key escrow

The VeriSign DOD IECA will establish its subscribers with a "dual-use" certificate (that is, the private key will be certified for both encryption and digital signature). The VeriSign DOD IECA will neither offer nor provide a key recovery service for such keys.

### 6.2.4 Private key backup

VeriSign DOD IECA subscribers are obligated to prevent unauthorized disclosure of their private keys. This includes any means undertaken to establish a backup copy of the key pair in support of disaster recovery.

Backup copies of the VeriSign DOD IECA private key are made to facilitate disaster recovery. These copies are maintained in secure facilities and are subject to the same access control policies and practices established for the operational copy.

The process by which a backup copy of the VeriSign DOD IECA key pair is made ensures that the private key never leaves the hardware protection boundary established during the original Key Ceremony process. The hardware tokens VeriSign deploys for these purposes enable strong cryptographic authentication of a recipient token as a legitimate token to receive a backup copy. Once this authentication is established, the program VeriSign uses to control the process will activate the source token and the destination token to create a one-time shared 3DES encryption key, which is used to protect the private key while in transit from the source token to the destination token.

The value of this encryption key is known only to the tokens themselves. It is never exposed to the software that controls the process.

#### 6.2.5 Private key archival

The VeriSign DOD IECA does not accept subscriber private keys for archival purposes.

#### 6.2.6 Private key entry into cryptographic module

When the VeriSign DOD IECA makes a backup copy of its private key, the key is transferred to hardware token in encrypted form. At no time does the key exist in plain-text form outside the hardware protection boundary.

Subscribers may use the secure export/import capability in the latest versions of the browsers to securely transfer key and certificates via the PKCS#12 protocol.

#### 6.2.7 Method of activating private key

The VeriSign DOD IECA hardware token utilizes a PIN-based activation mechanism. This PIN is generated during initialization of the token and split into shares for use in multi-party access control.

VeriSign DOD IECA subscribers are obligated to select a password during key generation. Entry of the password is required to activate the private key. The subscriber is the only entity that knows the password; at no time does the VeriSign DOD IECA become aware of the subscriber's password.

#### 6.2.8 Method of deactivating private key

The VeriSign DOD IECA hardware token is operated in a secured data center within an access-controlled secure facility. Access to the data center is strictly controlled. The token will deactivate its private key upon removal from its reader. When not in use, the token is stored in a vault.

#### 6.2.9 Method of destroying private key

In the event the VeriSign DOD IECA key requires destruction, the hardware token's "zeroize" command will be performed to do so.

### **6.3 Other Aspects Of Key Pair Management**

#### 6.3.1 Public Key Archival

The public key is archived as part of the certificate archival.

### 6.3.2 Usage Periods for the Public and Private Keys (*Key Replacement*)

The key usage periods for keying material is described in Section 7.

## **6.4 Activation Data**

### 6.4.1 Activation data generation and installation

VeriSign DOD IECA subscribers are requested to select their own password to protect their private key. Guidance regarding the select of a secure value is provided during the enrollment process.

The PIN used to protect the VeriSign DOD IECA and RA hardware tokens are randomly and automatically generated. Activation data protecting access to the IECA hardware token is generated within the FIPS 140-1 certified cryptographic module. The size of the activation PIN is 384 bits, exceeding that required by FIPS 112. Splitting it into several shares using the n-of-m scheme further protects the activation data.

### 6.4.2 Activation data protection

The VeriSign DOD IECA PIN is split into shares, each portion of which written to a separate non-volatile storage medium. Shares provided to selected trusted employees, one share per employee. Each individual so trusted maintains a separate secure lock box where the share under their control is stored when not in use. At no time is the value of a share, or the PIN, written down.

### 6.4.3 Other aspects of activation data

No stipulation.

## **6.5 Computer Security Controls**

### 6.5.1 Specific computer security technical requirements

The VeriSign DOD IECA employs an operating system that has been evaluated for security functionality, including audit requirements, identification and authentication, and discretionary access controls. This operating system is Sun Microsystems's Solaris, both 2.5.1 and 2.6.

Currently, several of the IECA operator accounts are not implemented to provide individual I&A. However, the DOD IECA has instituted sufficient system level and procedural controls to be able to effectively determine which authorized and trusted individual performed a security sensitive event. This is accomplished through strict personnel and procedural controls to limit these accounts to a few trusted individuals, and

is augmented by manual and automated perimeter controls that monitor (via active badges) which individuals have access to the system at any particular time.

### **6.5.2 Computer security rating**

VeriSign uses Sun Microsystems's Solaris operating system for production services. Currently, most systems operate with 2.6, though some still are operating with 2.5.1. Both Solaris 2.5.1 and 2.6 have been evaluated under the U.K. ITSEC program. 2.5.1 has been evaluated to E2, and 2.6 has been evaluated E3. VeriSign's databases use Oracle 7.3. Oracle 7 has been evaluated to C2 under TCSEC, and E2 under ITSEC. The VeriSign DOD IECA implements system-level controls that provide for identification and authentication, discretionary access controls, and audit of security critical events.

## **6.6 Life Cycle Technical Controls**

No stipulations.

## **6.7 Network Security Controls**

The VeriSign DOD IECA is designed to mitigate risk to external threats. Filtering at the routers is based on destination IP address and services. Firewalls use packet filtering and stateful inspection. The DMZ is segregated, with multiple firewalls internal and external to the DMZ. Communications with subscribers is encrypted using the SSL protocol.

The VeriSign DOD IECA firewall is configured such that all unused ports and services are turned off, only required user accounts are present, and only required network services software is installed.

Security monitoring is performed on the firewalls and critical servers. Throughout the day, automated scripts that test network response time, application status and application response times are run. Results are stored on a central logging host. Each shift has an assigned duty manager who is responsible for the first-line response in the event of system problems. Automated scripts notify Operations personnel if script results exceed specified parameters. Text messages describing the problem are sent to Operations personnel. Daily system management reports detailing disk and CPU usage, system load statistics, and system uptime are produced and stored centrally. These reports are maintained for the current and prior month.

Security monitoring tools used include:

- commercial security management products used for UNIX (e.g. ISS products)
- freely available UNIX security tools, including but not limited to:

- COPS and TAMU Tiger, for configuration management
- Crack, for checking weak passwords
- Tripwire, for checking file integrity and malicious code detection
- TCPWrapper, for controlling access to UNIX network services
- Nessus and SATAN for scanning for network issues

## **6.8 Cryptographic Module Engineering Controls**

See Section 6.2.

## 7 CERTIFICATE AND CRL PROFILES

The VeriSign DOD IECA will support two types of end-entity certificates. The first is a “dual-use” certificate to facilitate S/MIME interoperability and provide PKI-based access control with a single certificate. A single key will be certified for both signature and encryption.

The other is a “single-use” certificate used for digital signature purposes only.

The profiles of both certificate types are similar. The differences will be identified below.

### 7.1 Certificate Profile

This section identifies the essential characteristics of certificates that will be produced under this CPS. Appendix A of this CPS further establishes specific certificate content. At a minimum, certificates produced under this CPS will contain the following fields and indicated prescribed values or value constraints:

#### 7.1.1 Base Certificate

<u>Field</u>	<u>Value or Value constraint</u>
Version	(V3) 2
Serial Number	and MD5 hash
Issuer DN	C = US O = U.S. Government OU = DOD OU = PKI OU = Contractor OU = IECA-3 CN = VeriSign IECA
Subject DN	C = US O = U.S. Government OU = DOD

OU = PKI

OU = Contractor

OU = IECA-3

OU = Company Name

CN = name of subscriber + UID (unique UID per subscriber for all certificates)

Validity Interval CA: 3 years, end-entity: 1 year

Encoded IAW RFC2459

Subject Public Key rsaEncryption (1024 bits)

Algorithm Identifier: {1 2 840 113549 1 1 1}

encoded IAW RFC 2459

Signature sha-1WithRSAEncryption

Algorithm Identifier: {1 2 840 113549 1 1 5}

generated and encoded IAW RFC 2459

## 7.1.2 Use of Extensions

### 7.1.2.1 Basic Constraints

The certificates of CAs established under this CPS will contain a BasicConstraints extension with the CA field set to TRUE. The pathLengthConstraint field will not be included. The criticality field of this extension in CA certificates will be set to TRUE.

Individual subscriber certificates will contain a BasicConstraints extension with CA field assigned its default FALSE value. DER encoding rules establish that fields intended to be set to their default value shall be absent in the resulting encoding. Therefore, this field will be absent in the BasicConstraints extension individual subscriber certificates. The criticality field of this extension in end-entity certificates will be set to TRUE.

### 7.1.2.2 Key Usage

The certificates of CAs established under this CPS will contain a KeyUsage extension with the DigitalSignature, KeyCertSign and CRLSign bits set to 1 and all other bits set to 0. The criticality field of this extension in CA certificates will be set to TRUE.

Individual key encipherment subscriber certificates will contain a KeyUsage extension with the keyEncipherment bit set to 1 and all other bits set to 0. The criticality field of this extension in end-entity certificates will be set to TRUE.

Individual signature/authentication subscriber certificates will contain a KeyUsage extension with the digitalSignature and nonRepudiation bits set to 1 and all other bits set to 0. The criticality field of this extension in end-entity certificates will be set to TRUE.

### 7.1.2.3 Certificate Policies Extension

Both CA and end-entity certificates will contain a CertificatePolicies extension. This extension will be populated with the following value: {2 16 840 1 101 2 1 11 5}

The optional certificate policy qualifiers field of this extension will not be populated.

The criticality field of this extension will be set to its default value of FALSE.

### 7.1.2.4 Authority Key Identifier

Both CA and end-entity certificates will contain an AuthorityKeyIdentifier extension. The keyIdentifier field of this extension will be used to identify the authority key. This field will be populated with a 20-byte SHA-1 hash of the respective key IAW RFC2459. The criticality field of this extension will be set to FALSE.

### 7.1.2.5 Subject Key Identifier

Both CA and end-entity certificates will contain a SubjectKeyIdentifier extension. This extension will be populated with a 20-byte SHA-1 hash of the respective key IAW RFC2459. The criticality field of this extension will be set to FALSE.

### 7.1.2.6 Subject Alternate Name

All end entity certificates will contain a Subject Alternate Name extension populated with the end-user's RFC 822 email address. The criticality field of this extension is set to FALSE.

#### 7.1.2.7 CRL Distribution Points

All end entity certificates will contain a CRL Distribution Point extension encoded as URL=http://onsitecrl.verisign.com/USGovernment.../LatestCRL.crl. The criticality field of this extension is set to FALSE.

#### 7.1.3 Algorithm Object Identifiers

The VeriSign DOD IECA will issue certificates using the following OID for signatures in accordance with RFC2459:

Sha-1WithRSAEncryption: 1.2.840.113549.1.1.5

The VeriSign DOD IECA will issue certificates using the following OID for identifying the algorithm the subject key was generated for in accordance with RFC2459:

RsaEncryption: 1.2.840.113549.1.1.1

#### 7.1.4 Name Forms

See Section 7.1.1.

#### 7.1.5 Name Constraints

No stipulation.

#### 7.1.6 Certificate Policy Object Identifier

See Section 1.2.

#### 7.1.7 Usage of Policy Constraints

No stipulation.

#### 7.1.8 Policy Qualifiers Syntax and Semantics

The DOD IECA will not issue certificates that include policy qualifiers.

#### 7.1.9 Processing Semantics for the Critical Certificate Policy Extension

The DOD IECA will not mark the certificatePolicies as critical.

## **7.2 CRL Profile**

### 7.2.1 Version numbers

CRLs issued under this CPS will be version 1 CRLs. The VeriSign DOD IECA will not issue Authority Revocation Lists (ARLs) or any other partitioned CRLs.

### 7.2.2 CRL and CRL Entry Extensions

Since the CRLs are v1, there are consequently no CRL extensions or CRL entry extensions.

## **8 SPECIFICATION ADMINISTRATION**

### ***8.1 Specification Change Procedures***

Comments or issues with this CPS should be directed to the parties identified in section 1.4.2 of this document.

The DOD IECA PMA, prior to enactment, must approve material amendments to this CPS.

### ***8.2 Publication and Notification Procedures***

Upon approval of a CPS modification by the DOD PMA, an updated version of this document will be provided to the DOD PMA.

This VeriSign DOD IECA CPS is posted in the VeriSign repository at <http://www.verisign.com/repository/cps/dod/ieca.html>. Applicable updates to the IECA CPS that affect subscribers and relying parties will be posted on the VeriSign DOD IECA home page.

### ***8.3 CPS Approval Procedures***

The DOD PMA is the final approval authority of any proposed changes to this CPS.

### ***8.4 Waivers***

None required.

## **APPENDIX A - Definitions**

### **COMPROMISE**

A loss, theft, modification, or unauthorized access of a private key corresponding to the public key listed in a certificate governed by this CPS, including without limitation by cryptographic analysis or key extraction.

### **UNAUTHORIZED REVOCATION**

Revocation of a certificate without authorization of the subscriber by the subscriber's authorized agent except where VeriSign properly revokes the certificate under this CPS or the subscriber agreement with that subscriber.

### **LOSS OF USE**

The inability of a covered person to enter into a transaction due to the inability of the covered person or any user to securely access (loss of availability) a website or links from a website or databases within a website because of the inability of either the covered person (where the covered person is a subscriber) or the subscriber of a certificate issued under this CPS (where the covered person is relying on a subscriber's certificate) to use his/her/its certificate, or a covered person's inability to utilize or rely on indispensable certificate status services (such as online revocation or CRL services) to use a valid operational certificate in a timely fashion, caused by VeriSign.

### **ERRONEOUS ISSUANCE**

Issuance of a certificate in a manner not materially in accordance with the procedures required by the CPS, issuance of a certificate to a person other than the one named as the subject of the certificate, or issuance of a certificate without the authorization of the person named as the subject of such certificate. "Erroneous issuance" refers exclusively to certificates issued under this CPS.

### **IMPERSONATION**

Requesting and being issued a certificate issued under this CPS based on false or falsified information relating to naming or identity.

### **VERISIGN CERTIFICATE**

A certificate issued by VeriSign or any OnSite customer (whether or not it is a covered person under the Plan) as issuing authority and is of the class and type identified in

**[https://www.verisign.com/repository/ns\\_list](https://www.verisign.com/repository/ns_list)**. Certificates issued under this CPS are also VeriSign certificates.

**VERISIGN CERTIFICATION PRACTICE STATEMENT (CPS)**

The document, as revised from time to time, representing the VeriSign Trust Network's statement of the practices an IA within the VTN employs in issuing certificates. The VeriSign CPS is available:

(i) in electronic form within the VTN repository at **<https://www.verisign.com/cps>** and **<ftp://ftp.verisign.com/repository/CPS>**,

(ii) in electronic form via E-mail from **[CPS-requests@verisign.com](mailto:CPS-requests@verisign.com)**, and

(iii) in paper form from VeriSign, Inc., 1350 Charleston Road, Mountain View, CA 94043 USA, Attn: Certification Services.

**VERISIGN TRUST NETWORK (VTN)**

The certification system provided by VeriSign and any VeriSign-authorized IAs described in the VeriSign Certification Practice Statement.