VeriSign
External Certification Authority
Certification Practice Statement

Version 1.2

(Portions of this document have been redacted in accordance with the ECA Certificate Policy)

21 December 2007

VeriSign ECA Certification Practice Statement

Printed in the United States of America.

Revision Date: December 2007

Trademark Notices

VeriSign, Inc.

487 East Middlefield Road

Mountain View, CA 94043 USA

Attn: Practices Development.

Tel: +1 650.961.7500

Fax: +1-650-335-1077

eca-practices@verisign.com.

TABLE OF CONTENTS

1. INTRODUCTION 7

1.1 OVERVIEW 7
1.2 POLICY IDENTIFICATION 8
1.3 COMMUNITY AND APPLICABILITY 8
1.3.1 PKI Authorities 9
1.3.2. Trusted Entities 12
1.3.3 Related Authorities 13
1.3.4 End Entities 14
1.3.5 Applicability 14
1.4 CONTACT DETAILS 16
1.4.1 Specification Administration Organization 16
1.4.2 Contact Persons 16
1.4.3 Person Determining CPS Suitability for the Policy 17

2. GENERAL PROVISIONS 18

2.1 OBLIGATIONS 18
2.1.1 CA Obligations 18
2.1.2 RA Obligations 20
2.1.3 Trusted Agent Obligations 20
2.1.4 Subscriber Obligations 20
2.1.5 Relying Party Obligations 21
2.1.6 Repository Obligations 21
2.1.7 Certificate Status Authority Obligations 22
2.2 LIABILITY 22
2.2.1 Warranties and Limitations on Warranties 22
2.2.2 Disclaimers of Warranty and Liability 23
2.2.3 Limitations of Liability 24
2.2.4 Other Exclusions 24
2.2.5 US Federal Government Liability 25
2.3 FINANCIAL RESPONSIBILITY 25
2.3.1 Subscriber's Liability and Indemnity 25
2.3.2 Fiduciary Relationships 25
2.3.3 Administrative Processes 25
2.4 INTERPRETATION AND ENFORCEMENT 26
2.4.1 Interpretation 26
2.4.2 Severability, Survival, Merger, and Notice 27
2.4.3 Dispute Resolution Procedures and Choice of Forum 28
2.4.4 Successors and Assigns 29
2.4.5 No Waiver 29
2.4.6 Compliance with Export Laws and Regulations 29
2.4.7 Choice of Cryptographic Methods 29
2.4.8 Force Majeure 29
2.5 FEES 29
2.5.1 Certificate Issuance or Renewal Fees 29
2.5.2 Certificate Access Fees 30
2.5.3 Revocation or Status Information Access Fees 30
2.5.4 Fees for Other Services 30
2.5.5 Refund Policy 30
2.6 PUBLICATION AND REPOSITORIES 30
2.6.1 Publication of CA Information 30
2.6.2 Frequency of Publication 31
2.6.3 Access Controls 31
2.6.4 Repositories 31
2.7 COMPLIANCE AUDIT 32

2.7.1 Frequency of Compliance Audit *32*
2.7.2 Identity/Qualifications of Reviewer *32*
2.7.3 Auditor's Relationship to Audited Party *32*
2.7.4 Topics Covered by Compliance Audit *32*
2.7.5 Actions Taken as a Result of Deficiency *33*
2.7.6 Communication of Results *33*
2.8 CONFIDENTIALITY 33
2.8.1 Types of Information to Be Kept Confidential *33*
2.8.2 Information Release Circumstances *33*
2.9 INTELLECTUAL PROPERTY RIGHTS 33

3. IDENTIFICATION AND AUTHENTICATION 35

3.1 INITIAL REGISTRATION 35
3.1.1 Types of Names *35*
3.1.2 Need for Names to be Meaningful *35*
3.1.3 Rules for Interpreting Various Name Forms *35*
3.1.4 Uniqueness of Names *35*
3.1.5 Name Claim Dispute Procedure *35*
3.1.6 Recognition, authentication, and role of trademarks *35*
3.1.7 Method to prove possession of private key *36*
3.1.8 Authentication of Organization Identity *36*
3.1.9 Authentication of Individual Identity and Citizenship *36*
3.1.10 Authentication of Component Identities *39*
3.2 CERTIFICATE RENEWAL, UPDATE, AND ROUTINE RE-KEY 40
3.2.1 Certificate Re-key *40*
3.2.2 Certificate Renewal *41*
3.2.3 Certificate update *41*
3.3 RE-KEY AFTER REVOCATION 41
3.4 REVOCATION REQUEST 41

4. OPERATIONAL REQUIREMENTS 43

4.1 CERTIFICATE APPLICATION 43
4.1.1 Delivery of Subscriber's Public Key to Certificate Issuer *44*
4.2 CERTIFICATE ISSUANCE 44
4.2.1 Delivery of Subscriber's Private Key to Subscriber *45*
4.2.2 CA Public Key Delivery to Users *46*
4.3 Certificate Acceptance *46*
4.4 Certificate Suspension and Revocation *47*
4.4.1 Revocation *47*
4.4.2 Suspension *48*
4.4.3 Certificate Revocation Lists *49*
4.4.4 Online Status Checking *49*
4.4.5 Other Forms of Revocation Advertisements Available *49*
4.4.6 Special Requirements Related to Key Compromise *49*
4.5 SECURITY AUDIT PROCEDURES 49
4.5.1 Types of Events Recorded *49*
4.6 RECORDS ARCHIVAL 50
4.6.1 Types of Data Archived *50*
4.6.2 Retention Period for Archive *50*
4.7 KEY CHANGEOVER 50
4.8 COMPROMISE AND DISASTER RECOVERY 50
4.8.1 Compromise recovery *50*
4.8.2 Disaster Recovery *51*
4.9 CA TERMINATION 51

5. PHYSICAL, PROCEDURAL AND PERSONNEL SECURITY CONTROLS 52

5.1 PHYSICAL CONTROLS 52

5.2 PROCEDURAL CONTROLS 52
5.2.1 Trusted Roles *52*
5.2.1.5 Trusted Agent *52*
5.2.1.6 PKI Sponsor *52*
5.2.2 Separation of Roles *53*
5.3 PERSONNEL SECURITY CONTROLS 53
5.3.1 Background, Qualifications, Experience and Clearance Requirements *53*
5.3.2 Background Check Procedures *53*
5.3.3 Training Requirements *53*
5.3.4 Retraining Frequency and Requirements *54*
5.3.5 Job Rotation Frequency and Sequence *54*
5.3.6 Sanctions for Unauthorized Actions *54*
5.3.7 Contracting Personnel Requirements *54*
5.3.8 Documentation Supplied to Personnel *54*

6. TECHNICAL SECURITY CONTROLS 55

6.1 KEY PAIR GENERATION AND INSTALLATION 55
6.1.1 Key Pair Generation *55*
6.1.2 Private Key Delivery to Subscriber *55*
6.1.3 Key Sizes *55*
6.1.4 Public Key Parameters *55*
6.1.5 Parameter Quality Checking *55*
6.1.6 Hardware/Software Key Generation *55*
6.1.7 Key Usage Purposes *55*
6.2 PRIVATE KEY PROTECTION 56
6.2.1 Standards for cryptographic modules *56*
6.2.2 Private Key Multi-person Control *56*
6.2.3 Private Key Escrow *56*
6.2.4 Private Key backup *56*
6.2.5 Private Key Archival *56*
6.2.6 Private Key entry into cryptographic module *56*
6.2.7 Method of Activating Private Key *57*
6.2.8 Method of Deactivating Private Key *57*
6.2.9 Method of Destroying Private Key *57*
6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT 57
6.3.1 Public Key Archival *57*
6.3.2 Usage Periods for the Public and Private Keys *57*
6.4 ACTIVATION DATA 57
6.4.1 Activation data generation and installation *57*
6.4.3 Other aspects of activation data *58*
6.5 COMPUTER SECURITY CONTROLS 58
6.5.1 Specific computer security technical requirements *58*
6.5.2 Computer security rating *58*
6.6 LIFE CYCLE TECHNICAL CONTROLS 58
6.7 NETWORK SECURITY CONTROLS 58
6.8 CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS 58

7. CERTIFICATE AND CRL PROFILES 59

7.1 CERTIFICATE PROFILE 59
7.1.1 Version Numbers *59*
7.1.2 Certificate Extensions *59*
7.1.3 Algorithm Object Identifiers *59*
7.1.4 Name Forms *59*
7.1.5 Name Constraints *59*
7.1.6 Certificate Policy Object Identifier *59*
7.1.7 Usage of Policy Constraints *60*
7.1.8 Policy Qualifiers Syntax and Semantics *60*

7.1.9 Processing Semantics for the Critical Certificate Policy Extension *60*
7.2 CRL PROFILE 60
7.2.1 Version numbers *60*
7.2.2 CRL and CRL Entry Extensions *60*
7.3 OCSP REQUEST-RESPONSE FORMAT 60

8. SPECIFICATION ADMINISTRATION 61

8.1 SPECIFICATION CHANGE PROCEDURES 61
8.2 PUBLICATION AND NOTIFICATION PROCEDURES 61
8.3 CPS APPROVAL PROCEDURES 61
8.4 CPS WAIVERS 61

APPENDIX A: CERTIFICATE AND CRL PROFILES 62

A.1 ECA ROOT CA SELF-SIGNED CERTIFICATE 62
A.2 SUBORDINATE CA – CLIENT CERTIFICATE ISSUER 63
A.3 SUBORDINATE CA – COMPONENT CERTIFICATE ISSUER 64
A.4 IDENTITY CERTIFICATE 65
A.5 ENCRYPTION CERTIFICATE 67
A.6 COMPONENT CERTIFICATE 68
A.7 OCSP RESPONDER CERTIFICATE FOR CLIENT-ISSUING CA 69
A.8 OCSP RESPONDER CERTIFICATE FOR COMPONENT-ISSUING CA 70
A.9 SUBORDINATE CA CRL – FOR CLIENT-ISSUING CA 71
A.10 SUBORDINATE CA CRL – FOR COMPONENT-ISSUING CA 71

APPENDIX B: DEFINITIONS 72

APPENDIX C: IDENTITY PROOFING OUTSIDE THE U.S. 76

APPENDIX D: REFERENCES 80

APPENDIX E: ACRONYMS AND ABBREVIATIONS 81

APPENDIX F: VERISIGN ECA SUBSCRIBER AGREEMENT 82

1. INTRODUCTION

The Department of Defense (DOD) has identified the need for External Certification Authorities (ECAs) to provide PKI services for entities doing business with Federal, state and local government agencies. VeriSign is an approved External Certificate Authority operating under a Memorandum of Agreement (MOA) signed by the Assistant Secretary of Defense for Networks and Information Integration. The VeriSign ECA provides X.509 digital certificates for entities such as individuals, contractors and external organizations to enable secure, interoperable communications with the DOD and other Federal, state and local government organizations.

Following successful deployment and evaluation of Interim Electronic Certificate Authorities (IECAs), the DOD established requirements for the ECA program. This VeriSign ECA Certification Practice Statement (CPS), in conjunction with the ECA Memorandum of Agreement (MOA) and the Certificate Policy (CP) for External Certificate Authorities (version 3.1, 30 August 2006) defines the practices that VeriSign will employ in issuing and managing certificates and in maintaining a certificate-based public key infrastructure (PKI) for the ECA. This VeriSign ECA CPS is posted in the VeriSign repository at https://www.verisign.com/repository.

1.1 OVERVIEW

This CPS is the statement of practices that VeriSign will employ when issuing digital certificates as an approved ECA. This CPS is structured in accordance with RFC 2527 of the Internet Engineering Task Force (IETF). The VeriSign ECA service offering provides complete certificate life-cycle support and certificate repository services for approved entities. VeriSign has established an ECA that is subordinate to the ECA Root CA. The ECA Root CA serves as the "trust anchor" for all certificates issued by the VeriSign ECA. The architecture and functional solution for the VeriSign ECA is based on VeriSign's managed PKI service offering which has been deployed at numerous government agencies, and also has been approved for cross-certification with the Federal Bridge Certification Authority (FBCA) at the Medium assurance level.

The VeriSign ECA primary location is at the VeriSign data center located in Mountain View, California. A disaster recovery site with full backup and data mirroring is located in Virginia. All customer transactions are copied between the primary and disaster recovery systems in real-time over a secure VPN connection.

Authorized VeriSign personnel will perform the Certification Authority (CA) and Registration Authority (RA) functions as described in this CPS. The RA, however, will rely on a delegated in-person identity proofing process performed by public notaries or authorized Trusted Agents. For organizations that enter into a contract with VeriSign for a large volume of certificates, the RA or TA functions may be delegated to representatives of the organization.

End-entities supported by the VeriSign ECA are US Government contractors and external organizations needing to transact secure electronic business with the DOD or other Federal, State or Local government organizations. The VeriSign ECA will issue X.509 Version 3 certificates

compliant with the certificate profiles listed in the ECA Certificate Policy. The certificates can be used by the Subscribers and relying parties 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.

1.2 POLICY IDENTIFICATION

This CPS describes VeriSign's ECA practices for PKI services delivered in accordance with the ECA MOA and the ECA Certificate Policy.

The VeriSign ECA is a certification authority subordinate to the ECA Root. The ECA CP defines certificates at two assurance levels: medium and medium hardware. The object identifiers (OIDs) for these assurance levels, which are registered under Computer Security Objects Registry (CSOR) maintained by the National Institute of Standards and Technology (NIST), are as follows:

{joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101)csor(3)pki(2) cert-policy(1)eca-policies(12)

id-eca-medium	ID={id-eca-policies 1}
id-eca-medium-hardware	ID={id-eca-policies 2}

The VeriSign ECA issues certificates at the medium and medium hardware assurance levels.

1.3 COMMUNITY AND APPLICABILITY

This CPS as well as the ECA CP describes a PKI for individuals and organizations transacting business electronically with the DOD and other government agencies. This CPS describes the rights and obligations of persons and entities authorized under this CPS and the ECA Certificate Policy to fulfill any of the following roles: Certification Authority, Registration Authority, Notary, Trusted Agent, Repository, Certificate Status Authority and the end-entity roles of Subscriber and Relying Party.

The ECA Certificate Policy defines the requirements for the creation and management of X.509 Version 3 public-key certificates for use in applications requiring communication between networked computer-based systems. These applications include, but are not limited to: electronic mail; transmission of unclassified information; signature of electronic forms; contract formation signatures, signatures on mobile code in order to verify the integrity and source of mobile code; and authentication of infrastructure components such as web servers, firewall and directories. The intended network for these network security applications is the Internet.

1.3.1 PKI Authorities

1.3.1.1 Policy Management Authority

The ECA Policy Management Authority (EPMA) was established by the DOD to support the ECA program with the following responsibilities:

- Oversee the creation and update of the ECA CP and plans for implementing any accepted changes;
- Provide timely and responsive coordination to approved ECAs and Government Agencies through a consensus-building process;
- Review and approve the Certification Practice Statements (CPS) of CAs that offer to provide services meeting the requirements of the ECA CP; and
- Review and approve the results of CA compliance audits to determine if the CAs are adequately meeting the requirements of the ECA CP and associated approved CPS documents, and make recommendations to the CAs regarding corrective actions, or other measures that might be appropriate, such as revocation of CA certificates or changes to this CPS.

1.3.1.2 Certification Authority (CA)

The VeriSign ECA is an entity authorized by the EPMA to create, sign and issue digital certificates that conform to the requirements of the ECA CP and this CPS. The VeriSign ECA shall implement two (2) Certification Authorities subordinate to the ECA Root CA for the issuance of client and component certificates, respectively. The ECA Root CA serves as the "trust anchor" for certificates issued by the VeriSign ECA. The VeriSign ECA is operated at VeriSign's primary data center in Mountain View, California. The VeriSign ECA is subordinate to the US Government ECA Root CA. The VeriSign ECA issues all end-entity certificates within the VeriSign ECA domain. Figure 1 illustrates the ECA PKI hierarchy.

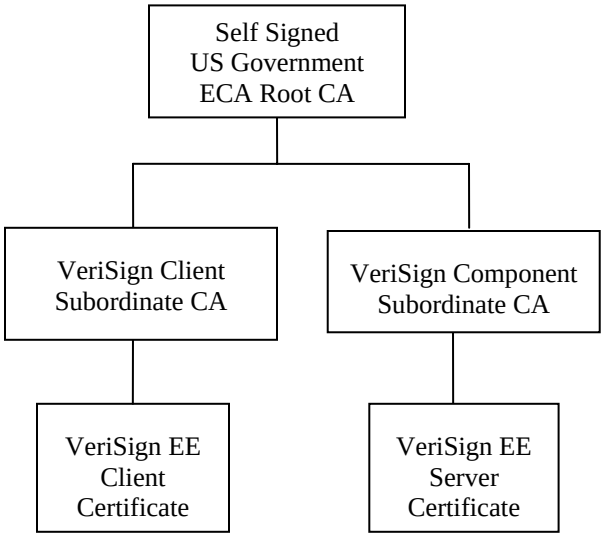

Figure 1. ECA PKI for VeriSign

The VeriSign ECA CA is responsible for all aspects of the issuance and management of ECA certificates, including control over the registration process, the identification and authentication process, the certificate management process, publication of certification, revocation of certificates and re-key; and for ensuring that all aspects of the CA services and CA operations and infrastructure related to ECA certificates are performed in accordance with the requirements, representations, and warranties of this CPS.

1.3.1.3 Registration Authority (RA)

VeriSign personnel and designated Company RAs will perform the RA functions for the VeriSign ECA. The VeriSign ECA maintains the list of approved RAs. A person may be approved as a RA upon completion of the following steps: 1) If a Company RA, after the RA's organization enters into an agreement with VeriSign and identifies the specific individuals authorized by the organization to be RAs; 2) The RA signs and submits a RA Authorization Form to VeriSign; and 3) The RA successfully enrolls for a certificate. VeriSign RA personnel are co-located with the CA, at the VeriSign secure data facility in Mountain View, CA.

For ECA certificate applicants located in the U.S., the RA relies on an in-person identity validation process performed by a Notary Public or Trusted Agent. For ECA certificate applicants located outside the U.S., the RA relies on an in-person identity validation process performed by a U.S. consular officer or an authorized DOD employee as specified in Appendix C of this CPS .

VeriSign will establish a contractual relationship with an organization prior to the authorization of a Trusted Agent to perform identity verification of employees/entities of the company. The

VeriSign ECA 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 ECA RA is a VeriSign trusted person operating a dedicated RA workstation within VeriSign’s secure facilities on VeriSign’s internal corporate network. VeriSign ECA RA personnel are issued public key certificates to enable secure authenticated access to the ECA. The ECA RA certificate is stored on a FIPS 140-1/2 level 2 hardware token. VeriSign may authorize organizations to appoint Company RAs to perform RA functions on behalf of employees of their affiliated company/organization. A Company RA is an employee of an organization that has entered into a contract with VeriSign for the purchase of a high volume of certificates for its employees/affiliates. The Company RA will be bound by the agreement between VeriSign and the organization to comply with the requirements of the ECA CP and this CPS. Company RAs will be issued public key certificates to enable secure authenticated access to the ECA. The Company RA certificate is stored on a FIPS 140-1/2 level 2 hardware token. The Company RA will operate a dedicated workstation on the Company’s internal network protected by a firewall, anti-virus software and other appropriate network security measures and maintained in a locked facility.

1.3.1.4 Certificate Management Authority

The VeriSign ECA CA, RAs and Company RAs are considered “Certificate Management Authorities” (CMAs) as defined in the ECA CP. The term CMA refers to a function assigned to either CAs or RAs, or to both CAs and RAs.

Server based Certificate Status Authorities (CSAs) such as Online Certificate Status Protocol (OCSP) Responders operated by an ECA vendor are also considered CMAs. VeriSign will operate an OCSP Responder for the ECA.

VeriSign is responsible for ensuring that all VeriSign ECA CMAs (i.e., the CA, CSAs, RAs, and Company RAs) are in compliance with this CPS and the ECA CP.

1.3.1.5 Repository

VeriSign will operate the ECA Repository from its secure data facility located in Mountain View, California. This Lightweight Directory Access Protocol (LDAP)-compliant directory contains ECA Subscriber certificates and Certificate Revocation Lists (CRLs) and the VeriSign ECA certificate and associated CRL.
Updates to information contained in the VeriSign ECA repository shall be controlled via certificate-based access over SSL and shall be limited to authorized VeriSign personnel and processes. Subscribers and relying parties may query, view, and download certificate and CRL entries in the repository via an https or LDAP query.

1.3.2. Trusted Entities

1.3.2.1 Notaries

For U.S citizens and non-U.S. citizens located in the U.S, the VeriSign ECA relies on the identity proofing services of State and Federal appointed public notaries. Public notaries validate the identities of Subscribers who are unable to appear before a VeriSign RA, Company RA or Trusted Agent. A Notary Public is responsible for validating a Subscriber's identity, citizenship and company/organizational affiliation based on the presentation of a government-issued photo ID and other credentials identifying organizational affiliation. The Notary Public also witnesses the Subscriber signature on the Subscriber Enrollment Form, which acknowledges the Subscriber's responsibilities and obligations as an ECA certificate holder and attests to the truth of the information in the Subscriber Enrollment Form. The notary attests to these acts by signing the Subscriber's enrollment form and applying his or her seal/stamp.

1.3.2.2 Consular Officer

Consular officers at U.S. embassies and consulates abroad have the authority to perform any notarial act which any public notary within the United States is authorized by law to do. Consular officers may act as notaries public for the purpose of performing identity proofing of ECA certificate applications (both U.S. and non-U.S. citizens) located outside the U.S. A consular officer is responsible for validating a Subscriber's identity and citizenship based on the presentation of a valid government-issued photo ID and a valid passport. Specific requirements for identity proofing by consular officers are contained in Appendix C of this CPS.

1.3.2.3 Trusted Agent

A Trusted Agent is a person authorized to act as a representative of the RA in providing Subscriber identity proofing during the enrollment process. The VeriSign RA maintains the list of approved Trusted Agents. A person may be approved as a Trusted Agent after completion of the following steps: 1) The Trusted Agent's organization enters into an agreement with VeriSign and identifies the specific individuals authorized by the organization to be Trusted Agents; 2) The Trusted Agent signs and submits a Trusted Agent Authorization Form to VeriSign; and 3) The Trusted Agent successfully enrolls for an ECA certificate. Authorized employees of VeriSign or its affiliates and US federal, state and local government employees may also serve as Trusted Agents.

Trusted Agents must submit an enrollment for an ECA Subscriber certificate. Trusted Agents who are enrolling to perform identity proofing for Medium Assurance ECA certificates may appear before a Notary for identity proofing. Trusted Agents who are enrolling to perform identity proofing for Medium Hardware Assurance ECA certificates must appear before a VeriSign RA for identity proofing. Trusted Agents are holders of ECA Subscriber certificates and are considered agents of VeriSign, but they do not have privileged access to ECA functions. A Trusted Agent is responsible for validating a Subscriber's identity, citizenship and organizational affiliation based on the presentation of a government-issued photo ID and other identity documents. The Trusted Agent also witnesses the Subscriber signature on the Subscriber

Enrollment Form, which acknowledges the Subscriber's responsibilities and obligations as an ECA certificate holder and attests to the truth of the information in the Subscriber Enrollment Form. The Trusted Agent attests to these acts by signing the Subscriber Enrollment Form. Trusted Agents are responsible for archiving signed Subscriber Enrollment Forms. The Trusted Agent enters Subscriber enrollment information on a bulk submittal form that is digitally signed, encrypted and e-mailed to the VeriSign ECA RA. The VeriSign ECA RA shall validate submissions from Trusted Agents by verifying the digital signature on the bulk submittal form and checking that the submitter is on the list of approved Trusted Agents.

1.3.2.4 Organizational Representative

The VeriSign ECA validates that a Subscriber is affiliated with the organization identified on the Subscriber's enrollment form either by relying on an attestation signed both by the Subscriber and a representative of the Subscriber's organization or by inspecting a photo ID showing organizational affiliation. The Subscriber enrollment form has a section that must be signed by an authorized organizational representative (e.g. HR person) to attest to the Subscriber's organizational affiliation, and to indicate the organization's approval for the named Subscriber to use the resulting certificate. The VeriSign ECA RA verifies the consistency between the name on the notarized enrollment form and the name on the Subscriber's electronic certificate application and also validates the identity of the organizational representative (see Section 3.1.8). In addition, the VeriSign ECA RA will query external databases (e.g. Dun & Bradstreet database) to verify the existence and legitimate name of the organization identified on the Subscriber enrollment form.

1.3.2.5 Authorized DOD Employees (outside the U.S.)

The VeriSign ECA may rely upon authorized DOD employees to perform identity proofing and citizenship verification of non-U.S. citizens located outside the U.S. Specific requirements for identity proofing by authorized DOD employees are contained in Appendix C of this CPS.

1.3.3 Related Authorities

1.3.3.1 Compliance Auditor

VeriSign retains the services of an independent security auditing firm, (e.g. KPMG), which conducts a yearly examination of the controls associated with VeriSign's operations as set forth in VeriSign's practices documentation. The 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.

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

1.3.4 End Entities

1.3.4.1 Subscribers

An ECA Subscriber is an entity whose name appears as the subject in an ECA certificate, and who asserts that it uses its key and certificate in accordance with ECA policy. ECA Subscribers are limited to the following categories of entities:

- Employees of businesses acting in the capacity of an employee and conducting business with a US government agency at local, state or Federal level;
- Employees of state and local governments conducting business with a US government agency at local, state or Federal level;
- Employees of foreign governments or organizations conducting business with a US Government agency at local, state or Federal level;
- Individuals communicating securely with a US government agency at local, state or Federal level; and
- Workstations, guards and firewalls, routers, trusted servers (e.g., database, FTP, and WWW), and other infrastructure components communicating securely with or for a US government agency at local, state or Federal level. These components must be under the control of humans, who accept the certificate and are responsible for the correct protection and use of the associated private key.

Although the ECA is a Subscriber, the term Subscriber as used in this document refers only to those who request certificates for uses other than signing and issuing certificates.

1.3.4.2 Relying Parties

A Relying Party is the entity who, by using another's certificate to verify the integrity of a digitally signed message, to identify the creator of a message, or to establish confidential communications with the holder of the certificate, relies on the validity of the certificate that binds the Subscriber's name to a public key. A Relying Party may use information in the certificate (such as certificate policy identifiers) to determine the suitability of the certificate for a particular use and does so at their own risk. An ECA relying party is an individual or application that accepts a secure transaction from an ECA Subscriber.

1.3.5 Applicability

The ECA is intended to support the following security services: *confidentiality, integrity, authentication* and *technical non-repudiation.* It supports these security services by providing Identification and Authentication (I&A), integrity, and technical non-repudiation through digital signatures, and confidentiality through key exchange. These basic security services support the long-term integrity of application data, but may not by themselves provide a sufficient integrity

solution for all application circumstances. For example, when a requirement exists to verify the authenticity of a signature beyond the certificate validity period, such as contracting, other services such as trusted archival services or trusted timestamp may be necessary. These solutions are application based, and must be addressed by Subscribers and Relying Parties. The ECA provides public key certificates to support security services for a wide range of applications that protect various types of information, up to and including sensitive unclassified information.

Certificates issued under this CPS are not designed, intended, or authorized for use 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.

1.3.5.1 Level of Assurance

The level of assurance associated with a public key certificate is an assertion by a CA of the degree of confidence that a Relying Party may reasonably place in the binding of a Subscriber's public key to the identity and privileges asserted in the certificate. Assurance level depends on the proper registration of Subscribers and the proper generation and management of the certificate and associated private keys, in accordance with the requirements of the policy asserted in the certificate. Personnel, physical, procedural, and technical security controls contribute to the assurance level of the certificates issued by a certificate management system.

1.3.5.2 Factors in Determining Usage

The amount of reliance a relying party chooses to place on an ECA certificate should be determined by analysis of various risk factors. Specifically, the value of the information, the threat environment, and the existing protection of the information environment should be used to determine the appropriate level of assurance of certificates required to protect and authenticate the information.

1.3.5.3 Threat

Threat is any circumstance or event with the potential to cause harm. In terms of information systems, harm includes destruction, disclosure, or modification of data, processes, or processing components. Threats to systems include environmental disasters, physical damage, system penetration, violation of authorization, human error, and communications monitoring or tampering.

1.3.5.4 General Usage

The ECA CP defines two different levels of assurance, and provides guidance for their application. The choice of appropriate assurance level should be based on value of the information to be protected and an analysis of the existing protection of the information environment. Emphasis is placed on two types of activity: integrity and access control to information considered sensitive, and information related to electronic financial transactions and other e-commerce. The final selection of the security mechanisms and level of strength and

assurance requires a risk management process that addresses the specific mission and environment. This risk analysis should be carried out by each relying party.

Medium Assurance: This level is intended for applications handling sensitive medium value information, with the exception of transactions involving issuance or acceptance of contracts and contract modifications. Examples of medium assurance applications include:

- Non-repudiation for small and medium value financial transactions other than transactions involving issuance or acceptance of contracts and contract modifications;
- Authorization of payment for small and medium value financial transactions;
- Authorization of payment for small and medium value travel claims;
- Authorization of payment for small and medium value payroll; and
- Acceptance of payment for small and medium value financial transactions.

Medium Hardware Assurance: This level is intended for all applications operating in environments appropriate for medium assurance but which require a higher degree of assurance and technical non-repudiation.

- All applications appropriate for medium assurance certificates; and
- Applications performing contracting and contract modifications

1.4 CONTACT DETAILS

1.4.1 Specification Administration Organization

The organization responsible for administering this CPS is the VeriSign Practices Development group. Questions or correspondence related to this CPS should be addressed as follows:

VeriSign, Inc.
487 East Middlefield Road
Mountain View, CA 94043 USA
Attn: Practices Development – CPS
+1-650 961-7500 (voice)
+1-650-335-1077 (fax)
eca-practices@verisign.com

1.4.2 Contact Persons

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

Nicholas Piazzola
VeriSign, Inc.
605 Shipley Road

Linthicum, MD 21090
410-691-2100
npiazzola@verisign.com

1.4.3 Person Determining CPS Suitability for the Policy

The ECA Policy Management Authority (EPMA) determines the suitability of the VeriSign ECA CPS and its compliance with the ECA 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 PKI described in this CPS. These parties are:

- Certification Authority
- Registration Authority
- Trusted Agent
- Subscriber
- Relying Party
- Repository
- Certificate Status Authority

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:

- Upon publication of this CPS in the case of the CA, RA, Trusted Agent, CSA, and Repository;
- Upon submission of an application for a certificate, in the case of a Subscriber; and
- 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 and the Subscriber Agreement.

2.1 OBLIGATIONS

2.1.1 CA Obligations

The VeriSign ECA is obligated to all that rely on the information contained in the certificate to ensure that the certificate was issued to the named Subscriber as witnessed by the notary or trusted agent, that the information in the certificate is accurate and consistent with the identity information so witnessed by the notary or trusted agent (including, but not limited to the Subscriber's Distinguished Name in the subject field and the subject public key information field), and that the Subscriber has accepted the certificate.

The VeriSign ECA is obligated to ensure that the Subscriber who is the subject of the certificate is notified that the certificate has been issued. Direct notification to the Subscriber is

accomplished through an HTML form or via e-mail. In addition, all ECA Subscriber certificates are published to the VeriSign ECA repository. Separate query pages are provided to enable the download of Identity and Encryption certificates.

The VeriSign ECA 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 ECA and posted to the VeriSign ECA Repository**.** The VeriSign ECA is obligated to notify Relying parties of the revocation of such Subscriber's certificate by the same means. Written notice including a reason for the revocation is also provided to a Subscriber whose certificate has been revoked.

The VeriSign ECA is obligated to maintain records necessary to support requests concerning its operation, including audit files and archives.

The VeriSign ECA shall issue certificates that assert either policy OID defined in this document and shall conform to the requirements of this document, including:

- Providing to the EPMA this CPS, as well as any subsequent changes, for compliance analysis and assessment;
- Conforming to the requirements of the ECA CP and this approved CPS;
- Ensuring that registration information is accepted only from RAs who understand and are obligated to comply with this policy. Note: Access control for ECA RAs is based on the name, e-mail address, organization and department listed in the ECA RA administrator certificate.
- Including only valid and appropriate information in the certificate, and maintaining evidence that due diligence was exercised in validating that information contained in the certificate;
- Ensuring that obligations are imposed on Subscribers in accordance with Section 2.1.4, and that Subscribers are informed of the consequences of not complying with those obligations;
- Revoking the certificates of Subscribers found to have acted in a manner counter to Subscriber obligations;
- Notifying Subscribers and making public for the benefit of Subscribers and Relying Parties any changes to the CA operations that may impact interoperability or security (e.g., extending the life of the self-signed root certificate);
- Operating or providing for the services of an on-line repository that satisfies the obligations under Section 2.1.6, and
- Posting certificates and CRLs to the repository.
- Check certificate validity before relying on any certificate.

2.1.2 RA Obligations

The VeriSign ECA RA and all Company RAs shall comply with the requirements of the ECA CP and this CPS. ECA RA obligations include the following: perform in-person identity proofing of ECA certificate applicants; witness and sign ECA Subscriber Enrollment Forms; archive signed ECA Subscriber Enrollment Forms; include only valid and appropriate information in ECA certificates; maintain evidence that due diligence was exercised in validating the information contained in ECA certificates; revoke the certificates of Subscribers in accordance with section 2.1.4; inform Subscribers of the consequences of not complying with the obligations in sections 2.1.4; check the consistency of the information contained within Subscriber Enrollment Forms either notarized by a Notary Public or witnessed by an authorized Trusted Agent; ensure that the Subscriber Enrollment Form contains appropriate attestation of the Subscriber's organizational affiliation; confirm the existence of the affiliated organization; and process requests and responses in a timely and secure manner. The VeriSign ECA RA and all Company RAs shall protect the RA private key in accordance with all applicable requirements of this CPS, including, but not limited to, those listed in section 6.2 of this CPS. The RA privileges of an RA found to have acted in a manner inconsistent with these obligations shall be revoked.

2.1.3 Trusted Agent Obligations

An ECA TA shall comply with the requirements of the ECA CP and this CPS. The ECA TA obligations include the following: enroll for an ECA certificate using the identity verification by notary process or by appearing before a VeriSign CMA; perform in-person identity proofing of ECA certificate applicants; witness and sign ECA Subscriber Enrollment Forms; archive signed ECA Subscriber Enrollment Forms; submit Subscriber enrollment data (Subscriber name, e-mail address and organizational affiliation) to the VeriSign ECA RA by electronically submitting bulk enrollment forms to VeriSign as an attachment to a digitally signed and encrypted e-mail. A TA may only request certificate revocation for a Subscriber whose identity was verified by that TA.

2.1.4 Subscriber Obligations

The following summarizes the obligations and responsibilities of an ECA certificate Subscriber:

Subscribers shall:

- Accurately represent themselves and ensure the accuracy of information provided in all communications with the ECA PKI;
- Protect their private keys at all times, in accordance with this CPS, and as set forth in the applicable Subscriber agreements;
- Notify the VeriSign ECA immediately if the Subscriber believes or has reason to believe that their private keys are compromised or lost. Such notification shall be made through mechanisms consistent with the ECA CP and this CPS;
- Notify the VeriSign ECA immediately if any of the information contained in the Subscriber's ECA certificate is no longer accurate or has changed.

- Abide by all the terms, conditions, and restrictions levied upon the use of their private keys and certificates.
- Agree not to monitor, interfere with, or reverse engineer the technical implementation of the VeriSign ECA except as explicitly permitted by this CPS or upon written approval by VeriSign.
- Agree not to submit to VeriSign or the VeriSign repository any materials that contain statements that are (i) libelous, defamatory, obscene, or pornographic, or (ii) otherwise violate any law.

PKI Sponsors (as described in Section 5.2.1) assume the obligations of Subscribers for the certificates associated with their components.

2.1.5 Relying Party Obligations

The following summarizes the obligations and responsibilities of parties who rely upon a certificate received from the VeriSign ECA repository or by other means:

- Perform a risk analysis to decide whether the level of assurance provided by the certificate is adequate to protect the Relying Party based upon the intended use;
- Use the certificate for the purpose for which it was issued, as indicated in the certificate information (e.g., the key usage extension);
- Check each certificate for validity, using procedures described in the X.509 standard [ISO 9594-8], prior to reliance;
- Establish trust in the CA who issued a certificate by verifying the certification path in accordance with the X.509 Version 3 Amendment;
- Preserve original signed data, the applications necessary to read and process that data, and the cryptographic applications needed to verify the digital signatures on that data for as long as it may be necessary to verify the signature on that data. Note: data format changes associated with application upgrades may invalidate digital signatures and shall be avoided.

2.1.6 Repository Obligations

The VeriSign ECA Repository is obligated to provide certificates, CRLs, and other revocation information for use by relying parties. The VeriSign ECA Repository shall maintain an availability of at least 99.5% per year for all components within its control. The VeriSign ECA Repository provides access control mechanisms sufficient to protect repository information as described in Section 2.6.3. The VeriSign repository is accessible via http query at https://eca.verisign.com and LDAP query at ldap://directory.verisign.com. VeriSign may publish both within and outside of the VeriSign repository a Subscriber's certificate and CRL-related data.

2.1.7 Certificate Status Authority Obligations

The VeriSign ECA CSA operates an OCSP responder that shall comply with the requirements of the ECA CP and this CPS. The VeriSign ECA CSA is obligated to ensure that certificate and revocation information is only accepted from the VeriSign ECA and that only valid and appropriate response is provided. The ECA CSA shall maintain evidence that due diligence was exercised in validating certificate status. A CSA who is found to have acted in a manner inconsistent with these obligations is subject to action as described in Section 2.7.5

2.2 LIABILITY

2.2.1 Warranties and Limitations on Warranties

This section sets forth the warranties, disclaimers of warranties, and limitations of liability provided by Certificate Authorities to Subscribers and Relying Parties pursuant to this CPS.

2.2.1.1 Certificate Authority Warranties

VeriSign, warrants to Subscribers that:

- There are no misrepresentations of fact in such certificate known to or originating from VeriSign;
- Any certificates issued that assert the policy OIDs identified in Section 1.2 are issued in accordance with the ECA CP and this CPS;
- There are no errors in the information in the certificate that were introduced by VeriSign as a result of its failure to exercise reasonable care in creating the certificate;
- Such certificate meets all requirements of this CPS; and
- Revocation services and use of a Repository conform to this CPS in all respects.

VeriSign warrants to Relying Parties who rely on a certificate that:

- All information in or incorporated by reference in such certificate is accurate;
- The certificate has been issued to the individual named in the certificate as the Subscriber; and
- VeriSign has complied with the ECA CP and this CPS when issuing the certificate.

2.2.1.2 RA Warranties

VeriSign performs both CA and RA functions and may authorize Company RAs to perform RA functions on behalf of their employees/affiliates. VeriSign warrants that any RA or Trusted Agent will operate in accordance with the applicable sections of the ECA CP and this CPS.

2.2.1.3 Subscribers' Representations

By accepting a ECA certificate issued by VeriSign, the Subscriber certifies to and agrees with VeriSign and to all who 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:

- 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 by the Subscriber and is operational (not expired, suspended or revoked) at the time the digital signature is created;
- the Subscriber has no knowledge of any unauthorized access to the Subscriber's private key;
- all representations made by the Subscriber to VeriSign regarding the information contained in the certificate are correct;
- all information contained in the certificate is correct to the extent that the Subscriber had knowledge or notice of such information and does not promptly notify VeriSign of any material inaccuracies in such information as set forth in CPS § 4.3.1;
- the certificate is being used exclusively for authorized and legal purposes, consistent with this CPS; and
- the Subscriber is an end-user and will not use or authorize any one to use the private key associated with the ECA certificate for signing any certificate or CRL.

By accepting a certificate, the Subscriber acknowledges that he/she agrees to the terms and conditions contained in the CP, this CPS and the applicable Subscriber agreement.

2.2.2 Disclaimers of Warranty and Liability

2.2.2.1 Specific Disclaimers

Except as otherwise set forth in the ECA CP and this CPS, VeriSign:

(a) Shall not incur liability to any person or entity for representations contained in a certificate, provided the certificate was prepared 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 or willful misconduct,
(b) Does 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
(c) Does 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 Warranty Disclaimer

EXCEPT AS SET FORTH IN THE ECA CP AND THIS CPS AND THE APPLICABLE SUBSCRIBER AGREEMENT, AND TO THE EXTENT PERMITTED BY APPLICABLE LAW, VERISIGN DISCLAIMS ANY AND ALL OTHER EXPRESS OR IMPLIED WARRANTIES OF ANY TYPE TO ANY PERSON OR ENTITY, 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.

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 this CPS and to the extent permitted by applicable law, VeriSign's liability shall be limited as follows:

The total liability of VeriSign to any party for general contract, tort or any other damages for negligent, reckless, or fraudulent conduct by the VeriSign ECA, its RAs or Trusted Agents in connection with a single transaction involving the use or reliance on a certificate shall be limited to one thousand dollars ($1,000 USD). Furthermore, VeriSign's total liability for any incident (aggregate of all transactions) involving the use or reliance on a certificate shall be limited to one million dollars ($1,000,000 USD). These liability caps 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.

2.2.3.2 Exclusion of Certain Elements of Damages

Except as expressly provided in this CPS, and to the extent permitted by applicable law, VeriSign shall not be liable in contract to any person or entity 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 or entity 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.

2.2.4 Other Exclusions

Not Applicable.

2.2.5 US Federal Government Liability

Subscribers and Relying Parties shall have no claim against the US Federal Government arising from use of the Subscriber's certificate or a CMA's determination to terminate a certificate. In no event will the Government be liable for any losses, including direct or indirect, incidental, consequential, special, or punitive damages, arising out of or relating to any certificate issued or revoked by the VeriSign ECA.

The VeriSign ECA shall have no claim for loss against the EPMA, including but not limited to the revocation of the ECA's certificate. Subscribers and relying parties shall have no claim against the US Federal Government arising from erroneous certificate status information provided by the servers and services operated by the ECA and by the U.S. Federal Government.

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 professional liability insurance.

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 VeriSign or any person receiving or relying on the certificate; or (iii) failure 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

The VeriSign ECA, RA or Company RA 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. VeriSign's financial resources are set forth in disclosures appearing at: http://corporate.verisign.com/investor/sec-filings.html

2.4 INTERPRETATION AND ENFORCEMENT

2.4.1 Interpretation

2.4.1.1 Governing Law

The relationship between this CPS and the ECA CP and the MOA between VeriSign and the EPMA shall be governed by the laws of the United States of America.

If you are an individual or entity within the United States Government and have purchased the services associated with this CPS, 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, 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 and the ECA CP except to the extent that the provisions of the ECA CP and this CPS are prohibited by law. In the event of a conflict between the ECA CP and this CPS, the ECA CP shall take precedence over this CPS.

2.4.1.3 Interpretation

Unless otherwise provided, this CPS shall be interpreted consistently with what is commercially reasonable under the circumstances, but only to the extent that what is commercially reasonable is consistent with the ECA CP.

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 §§ 2.2.2, 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 another person:	To the most recent address of record on file with VeriSign, Inc.

2.4.3 Dispute Resolution Procedures and Choice of Forum

The EPMA is the sole arbiter of disputes over the interpretation or applicability of the ECA CP.

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 and have purchased the services associated with this CPS, 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. 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 ECA 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.

2.4.8 Force Majeure

VeriSign shall not be responsible for any delay or failure in performance under this CPS that results from events beyond its control including, but not limited to, 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

VeriSign will publish its fees for ECA certificates on its web site at http://www.verisign.com/. Such fees are subject to change seven (7) days following their posting.

2.5.2 Certificate Access Fees

VeriSign ECA certificates shall be available to relying parties at no charge.

2.5.3 Revocation or Status Information Access Fees

VeriSign ECA certificate revocation lists (CRLs) shall be available to relying parties at no charge.

2.5.4 Fees for Other Services

The VeriSign ECA may charge a fee for key recovery services.

2.5.5 Refund Policy

The VeriSign ECA 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 that 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 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. Subscribers may request a refund in accordance with VeriSign's refund policy at http://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 ECA 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 ECA Subscriber certificates;
2) Certificate status information accessible by https and OCSP, and CRLs accessible by https and LDAP;
3) The most recently issued CRLs for the VeriSign ECA Client and Server CAs ;
4) The ECA Root CA certificate and the subordinate VeriSign ECA Client and Server CA certificate(s) needed to validate the signature on VeriSign ECA Subscriber certificates and CRLs;
5) Any other relevant information that VeriSign considers relevant regarding the use of VeriSign ECA certificates by its Subscribers or relying parties.
6) A copy of the Certificate Policy for External Certificate Authorities and an abridged version

of this CPS including at least the following topics covered under the ECA CP:

- Section 1.4, ECA Contact Information;
- Section 2, General Provisions;
- Section 3.1, Initial Registration;
- Section 4.4, Certificate Suspension and Revocation;
- Section 8, Certificate Policy Administration; and any additional information that the ECA deems to be of interest to the relying parties (e.g., mechanisms to disseminate ECA trust anchor, to provide notification of revocation of ECA root or ECA certificate).

The VeriSign ECA 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 ECA.

Upon the Subscriber's acceptance of the certificate, the VeriSign ECA shall immediately change the status field for the Subscriber in the VeriSign ECA Repository from pending to valid .

Upon revoking a certificate, the VeriSign ECA shall immediately change the status of the certificate indicated in the VeriSign ECA Repository from valid to revoked. The revoked status is immediately available via https or OCSP query.

CRLs will be created and published at least every eighteen (18) hours.

2.6.3 Access Controls

The VeriSign ECA shall not impose any read access restrictions to information published in its repository. Subscribers and relying parties may access certificate and CRL information via https, LDAP queries.

The VeriSign ECA shall protect any data in the repository (or data otherwise maintained by the ECA) that is not intended for public dissemination or modification. Updates to information contained in the VeriSign ECA repository shall be controlled via certificate-based access over SSL and shall be limited to authorized VeriSign ECA personnel.

2.6.4 Repositories

The VeriSign ECA Repository is implemented using LDAP technology. End users may search for ECA certificates and CRLs by https and LDAP and may query ECA certificate status by https and OCSP.

The VeriSign repository is accessible via http query at https://eca.verisign.com

The VeriSign Repository is accessible via LDAP query at ldap://directory.verisign.com

The CRL for the Client CA is available at http://eca-client-crl.verisign.com/VeriSignECA/LatestCRL.crl
The VeriSign Server CA CRL is available at https://eca-server-

crl.verisign.com/VeriSignECA/LatestCRL.crl

The VeriSign Client CA certificate is available at https://eca.verisign.com/CA/VeriSignECA.cer

The VeriSign Server CA certificate is available at https://eca.verisign.com/CA/VeriSignECASSL.cer

The ECA Root CA Certificate and the DOD PKI Root CA are available at https://eca.verisign.com/step2CAinstall.htm

2.7 COMPLIANCE AUDIT

2.7.1 Frequency of Compliance Audit

The VeriSign ECA shall undergo an annual compliance audit as part of its annual PKI audit, and will make itself available for additional compliance audits that may be required by the EPMA. The scope of the audits shall include the RAs and CSA. The VeriSign ECA also has the right to require aperiodic inspections of Company RA operations to validate that the Company RA is operating in accordance with the security practices and procedures described in the ECA CP and this CPS. Company RA operations will also be audited whenever the VeriSign ECA has reason to believe that the Company RA is not in compliance with this CPS.

2.7.2 Identity/Qualifications of Reviewer

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

2.7.3 Auditor's Relationship to Audited Party

The VeriSign ECA auditor is under a contractual relationship to VeriSign for its security audit services and has no role or responsibility relating to the VeriSign ECA operation. Representatives of VeriSign's IT Security/Audit department, who have no operation role or responsibility relating to the VeriSign ECA operation, will be responsible for auditing Company RAs.

2.7.4 Topics Covered by Compliance Audit

The Compliance Audit shall verify that VeriSign has in place a system to assure the quality of the ECA services that it provides and that the VeriSign ECA CA and the RAs comply with the requirements of the ECA CP and this CPS. All aspects of VeriSign's ECA and Company RA operations as specified in this CPS are subject to compliance audit inspections.

2.7.5 Actions Taken as a Result of Deficiency

Any discrepancies between the CMA operations and the requirements in this CPS will be immediately brought to the attention of the EPMA by the auditor. VeriSign will propose a remedy to the EPMA and provide an expected timeframe for completion.

Depending on the nature and severity of the discrepancy, the EPMA may decide to temporarily halt operation of the CA or RA, or to revoke the certificate.

2.7.6 Communication of Results

The compliance auditor shall report the results of a compliance audit to VeriSign and the EPMA. The implementation of remedies shall also be reported to the EPMA. A special compliance audit may be required to confirm the implementation and effectiveness of the remedy.

2.8 CONFIDENTIALITY

2.8.1 Types of Information to Be Kept Confidential

All non-certificate information received from Subscribers shall be treated as confidential by the VeriSign ECA and shall not be posted in the VeriSign repository. This information including: Dun and Bradstreet numbers, business or home addresses, telephone numbers and credit card data shall be handled as sensitive. This information will be stored locally on the ECA equipment and access will be limited to authorized personnel using certificate-based access control over client-authenticated SSL.

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

2.8.2 Information Release Circumstances

VeriSign will not disclose confidential information to any third party unless required by law, government rule or regulation, or order of a court of competent jurisdiction. VeriSign shall not release or be required to release any confidential information without an authenticated, reasonably specific request prior to such release.

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 and CRLs: Certificates and CRLs are the personal property of the VeriSign ECA. No fees will be levied on Relying Parties for access to VeriSign ECA certificates and CRLs.
- 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 ECA private keys are the personal property of VeriSign, Inc.
- VeriSign Public Keys: VeriSign ECA public keys are the property of VeriSign Inc. No fees will be levied on Relying Parties for access to VeriSign ECA public keys.

3. IDENTIFICATION AND AUTHENTICATION

3.1 INITIAL REGISTRATION

3.1.1 Types of Names

All certificates issued by the VeriSign ECA shall use the X.500 DN name format for subject and issuer name fields. Common Names shall be either Subscriber full name for individuals or URLs for web servers.

The DN format is: cn=<*Subscriber Name or URL*>, ou=<*Subscriber Company Name or Unaffiliated*>, ou=VeriSign, Inc., ou=ECA, o=U.S. Government, c=US

VeriSign ECA certificates may assert an alternate name form in the subjectAltName field.

3.1.2 Need for Names to be Meaningful

Certificates issued by the VeriSign ECA to humans will contain the legal name of the person to whom the certificate is issued and the company/organization name to which the Subscriber is affiliated. Certificates issued by the VeriSign ECA to web servers will contain the name and company/organizational affiliation of the person responsible for the web server (See Section 5.2.1.1 PKI Sponsor) and the domain name of the web server. The ECA CMA shall verify the affiliation between the Subscriber or PKI Sponsor and the company/organization identified in the certificate enrollment request.

3.1.3 Rules for Interpreting Various Name Forms

Rules for interpreting name forms are contained in the applicable certificate profiles (see Section 7.1.2. and Appendix A).

3.1.4 Uniqueness of Names

The VeriSign ECA will ensure the uniqueness of names for all certificates issued within the ECA domain. Information contained in certificate enrollment requests will be automatically checked against the VeriSign ECA database to prevent duplication and to ensure the uniqueness of the ECA certificate distinguished name and of the Subscriber e-mail address. Note: The VeriSign ECA database contains all past and current Subscribers. In the event of a name conflict, the VeriSign RA will reject the subscriber enrollment request and contact the subscriber to resolve the name conflict.

3.1.5 Name Claim Dispute Procedure

VeriSign shall investigate and correct, if necessary, any name collisions brought to its attention. If appropriate, VeriSign shall coordinate with and defer to the EPMA naming authority.

3.1.6 Recognition, authentication, and role of trademarks

The VeriSign ECA shall not knowingly issue a certificate including a name that a court of competent jurisdiction has determined infringes the trademark of another.

3.1.7 Method to prove possession of private key

For all Identity certificate requests in which the Subscriber generates the key pair in a web browser (medium assurance) or a FIPS 140-1/2 level 2 hardware token (medium-hardware assurance), the VeriSign ECA CA shall require proof of possession of the private key that corresponds to the public key in the certificate request. The technical mechanism to establish this proof is verification that the subscriber's enrollment request containing their public key is digitally signed with the corresponding private key. The VeriSign ECA will perform the digital signature verification check.

For Encryption certificate requests, the private key is generated by the VeriSign Key Manager on behalf of the Subscriber; hence proof of possession of the private key is not required. Secure delivery of the private key to the Subscriber is addressed in 4.2.1

3.1.8 Authentication of Organization Identity

A VeriSign ECA RA, Company RA or Trusted Agent shall validate the affiliation of the Subscriber with the organization. Additionally, the VeriSign ECA RA will ensure that a company's name is registered and that the company is registered to do business under that name. Proof of organizational affiliation shall be established by one of the following methods:

- The Subscriber may present an unexpired photo ID badge issued by the Subscriber's organization that indicates the Subscriber's organizational affiliation.
- The Subscriber may present an unexpired government-issued photo ID including the Subscriber's organizational affiliation.
- The Subscriber may present a Subscriber Enrollment Form with a signature from an organizational representative attesting to the Subscriber's organizational affiliation. Note: In this scenario the VeriSign ECA RA shall authenticate the organizational affiliation by placing a phone call to the registered (e.g. in D&B) phone number of the organization, or if the organizational representative has previously been identified by the organization to the VeriSign ECA RA and has an ECA certificate, by sending a signed e-mail.

3.1.9 Authentication of Individual Identity and Citizenship

The following requirements apply to applicants for ECA certificates (both U.S. citizens and non-U.S. citizens) located inside the U.S. Appendix C of this CPS specifies requirements for applicants for ECA certificates located outside the U.S.

Subscribers and PKI Sponsors are required to appear in person before a notary, authorized Trusted Agent, Company RA or VeriSign RA to validate their identity and citizenship prior to obtaining a certificate from the VeriSign ECA. The Subscriber must present two official identification credentials at least one of which must be a photo ID issued by a government authority with jurisdiction over the issuance of such credential for the applicant. The credential presented for identity verification must be a government issued photo ID such as a passport or driver's license or military identification. The credential presented for citizenship verification must be one of the following:

For non-US citizens, the only acceptable credential is a passport issued by the country of citizenship.

For US citizens, only the following credentials will be accepted:

- U.S. Passport
- Certified birth certificate issued by the city, county, or state of birth[1], in accordance with applicable local law
- Naturalization Certificate[2]
- Certificate of Citizenship[3]

The notary, RA, or Trusted Agent must review the identity documents and record the name, serial number, expiration date and type of identity document, date and sign the Subscriber Enrollment Form attesting to having authenticated the Subscriber's identity.

The notary, RA, or Trusted Agent will also witness that the Subscriber signs a Subscriber Enrollment Form 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 Subscriber Enrollment Form is accurate. VeriSign archives notarized Subscriber Enrollment Forms submitted by Subscribers. Company RAs, Trusted Agents and authorized DOD employees archive Subscriber Enrollment Forms for Subscribers whose identity and citizenship they have verified..

3.1.9.1 In-Person Authentication

For Medium Assurance, the applicant's identity and citizenship must be personally verified prior to the applicant's certificate issuance. The applicant shall appear personally before either:

- The VeriSign RA or an authorized Company RA
- A Trusted Agent formally approved by VeriSign;

---

[1] A certified birth certificate has a registrar's raised, embossed, impressed or multicolored seal, registrar's signature, and the date the certificate was filed with the registrar's office, which must be within 1 year of birth.

[2] A Naturalization Certificate is a document issued by U.S. Citizenship and Immigration Service (USCIS) since October 1, 1991 and the Federal Courts or certain State Courts on or before September 30, 1991 as proof of a person obtaining U.S. citizenship through naturalization.

[3] A Certificate of Citizenship is a document issued by U.S. Citizenship and Immigration Service (USCIS) is proof of a person having obtained U.S. citizenship through derivation or acquisition at birth (when born outside of the United States).

- A person certified by a US State or Federal Government as being authorized to confirm identities (such as Notaries Public), that uses a stamp, seal, or other mechanism to authenticate their identity confirmation
- The notary, RA, or Trusted Agent must review the identity documents and record the name, serial number, expiration date and type of identity document, date and sign the Subscriber Enrollment Form attesting to having authenticated the Subscriber's identity.
- The applicant shall appear before one of the required identity verifiers no more than thirty (30) days prior to application of the CA's signature to the applicant's certificate.

For Medium Hardware Assurance, the applicant's identity and citizenship shall be personally verified prior to the applicant's certificate being enabled. The applicant shall personally appear before either:

- the VeriSign RA or an authorized Company RA; or
- A Trusted Agent, only if the Trusted Agent's identity is personally verified by the VeriSign RA or a Company RA.
- The RA or Trusted Agent must review the identity documents and record the name, serial number, expiration date and type of identity document, date and sign the Subscriber Enrollment Form attesting to having authenticated the Subscriber's identity.

Minors and others not competent to perform face-to-face registration alone shall be accompanied by a person already certified by the VeriSign ECA , who will present information sufficient for registration at the level of the certificate being requested, for both himself and the person accompanied.

3.1.9.2 Electronic Authentication

The VeriSign ECA will issue certificates based on electronically authenticated (using a current, valid VeriSign ECA Identity certificate and associated private key) Subscriber requests, subject to the following restrictions. The VeriSign ECA shall maintain the information necessary to perform these checks in its database and shall perform the following checks:

- The assurance level of the new certificate shall be the same or lower than the assurance level of the existing certificate used as an authentication credential;
- The DN of the new certificate shall be identical to the DN of the certificate used as the authentication credential;
- Information in the new certificate that could be used for authorization shall be identical to that of the certificate used as the authentication credential;
- The expiration date of the new certificate shall be no later than the next required in-person authentication date associated with the certificate used as the authentication credential;
- The in-person authentication date associated with a new certificate shall be no later than the in-person authentication date associated with the certificate used for authentication; and
- The validity period of the new certificate shall not be greater than the maximum validity period requirements specified in this CPS for that type of certificate.

The VeriSign ECA supports electronic authentication for certificate re-key (see section 3.2.1).

3.1.10 Authentication of Component Identities

The VeriSign ECA will provide component certificates for use in web servers. Enrollment for the VeriSign ECA web server certificate must be performed by a human PKI Sponsor as described in Section 5.2.1.6. The PKI Sponsor is responsible for providing the ECA correct information regarding:

- Web Server domain name;
- Web Server public keys (using a Certificate Signing Request);
- Contact information to enable VeriSign to communicate with the PKI sponsor when required.

The VeriSign ECA requires in person registration of the PKI Sponsor, with the identity of the PKI Sponsor confirmed in accordance with the requirements of Section 3.1.9 as specified for ECA Subscribers. No equipment authorizations or attributes are included in the certificates.

The process for enrolling for an ECA Web Server certificate is as follows:

1) The PKI Sponsor will enter data on a SSL-protected web page for ECA Web Server certificate enrollment. This data will include the identification of the PKI sponsor, and affiliated organization information (e.g. Organization name and/or Dun and Bradstreet Number, an organizational point of contact and payment information.) The organizational point of contact must be able to confirm that the PKI Sponsor is affiliated with the organization and authorized to enroll for an ECA web server certificate on behalf of the organization. The VeriSign RA will place a call to the organizational contact using a registered phone number (e.g. in D&B) to confirm the affiliation of the PKI Sponsor.

2) The PKI Sponsor will also enter into the ECA web server enrollment form a Certificate Signing Request, which was previously generated on the web server.

3) The PKI Sponsor will enter a challenge password (not easily guessed and consisting of a minimum of 8 up to a maximum of 30 alpha-numeric characters) for the certificate enrollment and submit the enrollment request. The Subscriber must retain and protect the challenge password as it will be needed to download the ECA Web server certificate and can be later used by a CA or RA to authenticate the Subscriber (i.e. PKI Sponsor), if the Subscriber is requesting revocation of the certificate and cannot prove possession of the corresponding private key. The PKI Sponsor must then print the Subscriber Enrollment Form and take the form to a registered Notary Public or Trusted Agent.

4) The PKI Sponsor must appear in person before a Trusted Agent or registered Notary Public, and present two official identification credentials for identity and citizenship verification as described in section 3.1.9.1. The PKI sponsor must sign the Subscriber Enrollment Form in the presence of the Trusted Agent or Notary Public. In signing the Subscriber Enrollment Form, the PKI Sponsor attests that he or she is an employee of the organization indicated, that he or she is authorized to enroll for a certificate on behalf of the organization and that he or she has read and understands the Subscriber obligations of the ECA CP and CPS. If the PKI sponsor does not present a photo ID indicating company/organizational affiliation, the Subscriber Enrollment Form must also include a statement signed by a representative of the PKI Sponsor's affiliated company stating that the PKI Sponsor is an employee of the company and is authorized to enroll for an ECA certificate on behalf of the organization. The form must also contain proof of legal existence of the company (e.g. Dun and Bradstreet number). The Notary Public or Trusted Agent examines the two forms of identification,

records the type, identifying number and expiration date of each, and signs the form. The Notary Public also affixes his or her seal/stamp on the Subscriber enrollment form. The Trusted Agent may mail the signed registration form to VeriSign by first class postal mail, Federal Express, or other similar means. If verification is performed by a Notary Public, the Subscriber mails the form to VeriSign via first class postal mail, Federal Express, or other similar means.

5) After receiving the signed and witnessed Subscriber Enrollment Form, the VeriSign ECA RA performs the following checks:

a) Verification of consistency of the enrollment data on the Subscriber Enrollment Form with the enrollment data previously entered online by the PKI Sponsor.

b) Check of the validity of the domain name (e.g. via Internic query)

c) Check of the existence of the PKI Sponsor's organization (e.g. government database or Dun & Bradstreet query)

d) Verification of the PKI Sponsor's authorization (via telephone call to Organizational contact)

6) If all of the above checks are successful, the VeriSign ECA RA approves the web server certificate enrollment request and the ECA sends an e-mail to the PKI Sponsor with instructions and a PIN for downloading the web server certificate.

7) The PKI Sponsor goes to the URL provided in the e-mail, and in an SSL session enters the PIN (10 numeric digits) received in e-mail and the challenge password chosen during enrollment, and downloads the web server certificate.

3.2 CERTIFICATE RENEWAL, UPDATE, AND ROUTINE RE-KEY

3.2.1 Certificate Re-key

The VeriSign ECA supports re-key for Subscriber certificates. Re-keying a certificate means that a new certificate is created that is identical to the old one, except that the new certificate has a new, different public key (corresponding to a new, different private key); a different serial number; and may be assigned a different validity period.

Re-key requests for medium assurance certificates may be authenticated on the basis of existing Subscriber certificates (twice, up to a maximum of nine years for three year certificates), after which Subscribers must present themselves for in-person identity proofing, in accordance with Section 3.1. Re-key requests for medium hardware assurance certificates may be authenticated on the basis of existing Subscriber certificates. Every three years, in-person authentication is required, in accordance with Section 3.1.

An ECA Subscriber, whose certificates have not expired and whose initial Subscriber enrollment data has not changed, may re-key his or her certificates based on electronic authentication of a current, valid Identity certificate. The VeriSign ECA provides separate SSL-protected web pages for re-keying of Identity and Encryption certificates. The Subscriber must present his or her current Identity certificate in a client-authenticated SSL session. The VeriSign ECA validates the authenticity of the

certificate presented by verifying that the certificate was issued by the VeriSign ECA and comparing the subject name in the certificate to the corresponding certificate in the Repository. If the Subscriber meets the requirements for renewal noted above, the certificate will be renewed, otherwise the Subscriber will be directed to the in-person registration process identified in Section 3.1.

The VeriSign ECA may issue Subscriber certificates with one or three year lifetimes. The following are the maximum lifetimes for Subscriber certificates; ECA key lifetimes are provided in Section 4.7.

Medium Assurance	Identity certificate re-key every three years Encryption certificate re-key every three years May authenticate to PKI for re-key with current key twice
Medium Hardware Assurance	Identity certificate re-key every three years Encryption certificate re-key every three years Identity established in person

The VeriSign ECA shall issue OCSP responder certificates with a lifetime of one month.

3.2.2 Certificate Renewal

Renewing a certificate means creating a new certificate with the same name, key, and authorizations as the old one, but a new, extended validity period and a new serial number. The VeriSign ECA does not implement certificate renewal.

3.2.3 Certificate update

The VeriSign ECA does not implement certificate update.

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 ECA provides an online SSL-secured Web page at which Subscribers may request revocation of their ECA certificate(s). The Subscriber may request revocation of his or her certificate by sending a digitally signed e-mail message to the VeriSign RA. The VeriSign RA will authenticate the request by verifying the digital signature on the signed e-mail. Alternatively, if the Subscriber cannot authenticate using their private key, the Subscriber may authenticate by presenting his or her challenge password selected during the certificate enrollment process.

A Trusted Agent may request revocation of an affiliated Subscriber's certificate by sending a digitally signed e-mail message to VeriSign. The Trusted Agent shall authenticate the Subscriber's request for revocation by validating the Subscriber's identity in person, or by contacting an appropriate entity in the Subscriber's organization (e.g. HR representative). The VeriSign RA will authenticate the request received from the Trusted Agent by validating the digital signature on the signed e-mail and validating that the Trusted Agent is requesting revocation of a certificate for a Subscriber that is affiliated with his or her company.

A Company RA may revoke a Subscriber's certificate only for employees affiliated with his or her company. If the Company RA receives a revocation request from a Trusted Agent, the Company RA will authenticate the request as described above for the VeriSign RA. The Company RA shall authenticate the request for revocation and reason for revocation using the same procedures described above for Trusted Agents.

The VeriSign ECA RA or a Company RA may revoke a Subscriber's certificate for reasons that may include but not be limited to those identified in section 4.4.1.1.

4. OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

Applicants for both medium assurance and medium hardware certificates first connect to a VeriSign SSL-protected web page that includes general instructions for completing the certificate enrollment process. Applicants for medium hardware certificates must enroll in the presence of a VeriSign ECA RA or Company RA using the RA workstation. Each applicant completes an online certificate enrollment form and submits it as a request for a certificate. When the Subscriber submits the form, a dual key generation process is initiated. For medium assurance, the public-private key pair for the Identity certificate is generated locally on the on the Subscriber's workstation, and then the key pair for the Encryption certificate is generated in a VeriSign-hosted Key Manager Server crypto module. For medium hardware, the public-private key pair for the Identity certificate is generated locally on the Subscriber's hardware token, and then the key pair for the Encryption certificate is generated in the VeriSign-hosted Key Manager Server crypto module.

For Identity certificate enrollments, the VeriSign ECA verifies that the public key forms a functioning key pair with the private key held by the Subscriber as described in Section 3.1.7. The VeriSign ECA stores both certificate requests and posts a status of pending in the Repository. The VeriSign ECA presents the Subscriber with a pick-up password, which is twenty (20) randomly generated alpha-numeric characters that must be retained for later retrieving the Encryption certificate. Note: this password is required in addition to the 10 digit numeric pickup PIN that will be e-mailed to the Subscriber after the Subscriber Enrollment request is approved. The Subscriber then prints the Subscriber Enrollment Form containing the previously entered enrollment information. The Subscriber must then take the Subscriber Enrollment Form to a notary, trusted agent or an authorized company RA for in-person identity verification.

Identity Verification by Notary: A Subscriber must appear in person before a registered Notary Public and present two official identity credentials for identity and citizenship verification as described in section 3.1.9.1. The Subscriber must sign the Subscriber Enrollment Form in the presence of the Notary. One of the forms of ID may include a company or government-issued photo ID indicating the Subscriber's organization affiliation. Otherwise, the Subscriber Enrollment Form must include a statement signed by a representative of the Subscriber's affiliated company stating that the applicant is an employee of the company and is authorized to use an ECA certificate to secure the company's transactions with the DOD and other government agencies. The form must also contain proof of legal existence of the company (e.g. Dun and Bradstreet number or other proof of rights). The notary examines the two forms of identification, records the type, identifying number and expiration date of each, and affixes his or her seal/stamp on the Subscriber Enrollment Form. After the Notary processes the form, the Subscriber mails the notarized form to VeriSign via first class postal mail, Federal Express, or other similar means.

Identity Verification by Trusted Agent: A Subscriber may appear before an authorized Trusted Agent for in-person identity proofing and citizenship verification. Prior to performing in-person identity proofing of Subscribers, the Trusted Agent must first enroll for an ECA certificate using the Identity Verification by Notary process described above or by personally appearing before an RA. A Subscriber who appears before a Trusted Agent for identity proofing must present two forms of identification, including a government-issued photo ID (passport, driver's license or Military/DOD

identification card) and sign the Subscriber Enrollment Form. The second form of ID must include a company or government-issued photo ID indicating the Subscriber's organization affiliation. The Trusted Agent examines the two forms of identification and records the type, identifying number and expiration date of each. The Trusted Agent signs the Subscriber Enrollment Form that includes a statement that the applicant is an employee of the company and is authorized to use an ECA certificate to secure the company's transactions with the DOD and other government agencies. The Trusted Agent is responsible for archiving the signed Subscriber Enrollment Form . The Trusted Agent submits Subscriber enrollment data on a bulk submission form which is sent as an attachment to a digitally signed and encrypted e-mail.

Identity Verification by Company RA: An approved RA at a company will perform the same functions as the Trusted Agent described above. In addition, the RA will have only privileges to access and approve pending Subscriber enrollment requests and request revocation of certificates of employees of the RA's affiliated company. This capability is enforced by the VeriSign ECA.

Identity Verification by U.S. Consular Officer: See Appendix C of this CPS.

Identity Verification by Authorized DOD Employee: See Appendix C of this CPS.

4.1.1 Delivery of Subscriber's Public Key to Certificate Issuer

For medium assurance, the Subscriber's identity information and Identity public key are delivered to the certificate issuer simultaneously in an SSL-protected session. The format for the delivery of this data is dependent on the type of web browser used. For all browser types, the public key is signed by the corresponding private key as the mechanism to prove possession of the private key. On the Subscriber enrollment web page, Subscribers are notified that only FIPS 140-1/2 level 1 certified browsers should be used to enroll for an ECA certificate.

For medium hardware assurance, Subscribers use a FIPS 140-1/2 level 2 certified token for generating the Identity key pair and a FIPS 140-1/2 level 1 certified browser for delivering the Subscriber's identity and public key to the certificate issuer in an SSL-protected session.

For both medium assurance and medium hardware Encryption certificate requests, key pairs are generated at the CA; therefore, delivery of the public key to the certificate issuer is not required.

4.2 CERTIFICATE ISSUANCE

A pending certificate enrollment request may be approved by either the VeriSign ECA RA or a Company RA after successful in-person identity verification. In all cases the RA must check the validated data on the Subscriber Enrollment Form for consistency with the enrollment data previously entered online by the Subscriber before approving the request. The process for approving a Subscriber enrollment request is as follows.

Enrollment Approval-Notarized Forms: Each notarized Subscriber Enrollment Form is checked by the VeriSign ECA RA for consistency with the enrollment data that the Subscriber previously entered online and to ensure that the form has been signed by the Subscriber, witnessed by the Notary and that the notary seal has been applied to the form. The VeriSign ECA shall also verify that

organizational affiliation has been verified in accordance with section 3.1.8. The VeriSign ECA RA will also query various databases (e.g. Dun & Bradstreet) to verify the existence of the company with which the Subscriber is affiliated. After completion of these checks, the VeriSign RA approves the enrollment request and an e-mail is sent to the Subscriber with separate URLs and instructions for picking up the Identity and Encryption certificates, respectively.

Enrollment Approval-TA Bulk Submission Forms: For signed and encrypted bulk enrollment data received from Trusted Agents, the VeriSign ECA RA checks the validity of the digital signature on the Trusted Agent e-mail and confirms that the sender is an authorized Trusted Agent by comparing the subject name in the Trusted Agent certificate against a list of VeriSign RA-approved Trusted Agents. The VeriSign ECA RA then checks each Subscriber data record for consistency with the enrollment data previously entered online by the Subscriber, and that the Subscriber organizational affiliation is the same as that of the Trusted Agent. After completion of these checks, the VeriSign RA approves the enrollment request and an e-mail is sent to the Subscriber with two URLs, PINs and instructions for picking up the Identity and Encryption certificates.

Enrollment Approval-Company RA: Each Subscriber Enrollment Form witnessed and signed by the Company RA is checked for consistency with the Subscriber enrollment data previously entered online by the Subscriber. After completion of these checks, the Company RA accesses the VeriSign ECA control center and approves the enrollment request. Subsequently, an e-mail is sent to the Subscriber with two URLs, PINs and instructions for picking up the Identity and Encryption certificates.

Enrollment Approval-U.S. Consular Officer: See Appendix C of this CPS.

Enrollment Approval-Authorized DOD Employee: See Appendix C of this CPS.

After the RA approves a Subscriber enrollment request and the Subscriber receives the e-mail, the Subscriber goes online to an SSL-protected web page provided for retrieving the Identity certificate and enters the PIN provided in the e-mail received from the VeriSign ECA. If the PIN is correct, the ECA signs the pending certificate request and presents the Identity certificate for download into the web browser or hardware token. The Subscriber then goes to another SSL-protected web page provided for downloading the Encryption certificate, enters the PIN provided in the e-mail received from the VeriSign ECA and the pickup password provided at the time of enrollment. If the PIN and password are correct, the ECA signs the pending certificate request and presents the Encryption certificate in a PKCS#12 format for download into the web browser or hardware token. Note: the VeriSign ECA will lock out the Subscriber after 10 attempts in which a bad PIN or password is submitted. After each certificate is downloaded by the Subscriber, the ECA changes the status stored in the Repository from pending to approved.

4.2.1 Delivery of Subscriber's Private Key to Subscriber

Subscribers generate private Identity keys for medium assurance certificates in FIPS 140-1/2 level 1 software cryptographic modules (usually web browser certificate cache or other comparable

certificate store). For medium hardware certificates, Subscribers generate private Identity keys in FIPS 140-1/2 level 2 hardware cryptographic modules. For both certificate types since the Subscriber generates the key locally, there is no need to deliver the Subscriber's private key.

Private Encryption keys associated with both medium assurance and medium hardware certificates are generated in FIPS 140-1/2 level 2 hardware cryptographic modules and escrowed by the VeriSign ECA Key Manager. Immediately after escrowing of the private Encryption keys, all keying material is deleted from the Key Manager crypto module.

For medium assurance certificates, the private encryption keys are delivered in a PKCS#12 format to the Subscriber in an SSL-protected session. After the Subscriber successfully enters the PIN and password, the PKCS#12 file is downloaded to the Subscriber's workstation where it is decrypted by a FIPS 140-1/2 level 1 browser and stored in the browser cache. Prior to downloading the PKCS#12 file, the Subscriber is presented with a notice on the web page that advises the Subscriber that downloading the file by clicking on the download button constitutes acceptance of the private key.

For medium hardware assurance certificates, after the Subscriber successfully enters the PIN and password, the PKCS#12 file is downloaded to the RA's workstation where it is decrypted by the Aladdin token manager software and imported into the hardware token. Prior to downloading the PKCS#12 file, the Subscriber is presented with a notice on the web page that advises the Subscriber that downloading the file by clicking on the download button constitutes acceptance of the private key. After the private Encryption key is imported into the hardware token, the PKCS#12 file and password are erased by the token manager.

Only those authorized by VeriSign's ECA Key Recovery Practice Statement may access private keys associated with Encryption certificates.

4.2.2 CA Public Key Delivery to Users

The US Government ECA Root Certificate and the VeriSign ECA certificate shall be delivered to users and relying parties by downloading the certificates from a web site secured with a VeriSign Class 3 web server certificate. Subscribers will be required to compare the ECA Root Certificate hash against the hash value on a form received during the enrollment process or from a Trusted Agent, VeriSign RA or Company RA.

4.3 Certificate Acceptance

A Subscriber accepts a certificate when he or she downloads the certificate after successfully entering the required PINs at the SSL-protected web sites designated for downloading ECA Identity and Encryption certificates. At this time the status in the Repository is changed from pending to valid. The PINs for downloading the certificates are delivered to the Subscriber after an RA has approved the Subscriber enrollment request.

When a Subscriber completes the Subscriber Enrollment Form, they sign a statement on the Subscriber Enrollment Form declaring that they have read the Subscriber agreement and understand and accept their responsibilities as defined in Section 2.1.4. The Subscriber is also notified that the private key associated with their Encryption certificate is escrowed.

In the case of non-human components (web servers, routers, firewalls, etc.), the PKI Sponsor (as defined in Section 5.2.1.3) shall perform a similar function for the acceptance of the component certificate. There is no escrow of private keys associated with certificates for non-human components.

4.4 Certificate Suspension and Revocation

4.4.1 Revocation

4.4.1.1 Circumstances for Revocation

An ECA certificate shall be revoked when the binding between the subject and the subject's public key defined within the certificate is no longer considered valid. Circumstances for revoking a certificate shall include, but not be limited to:

- The Subscriber requests that his or her certificate be revoked;
- The Subscriber's company or organization requests that the certificate be revoked;
- A Company RA or Trusted Agent requests that the certificate be revoked.
- The certificate was mistakenly issued or obtained by fraud or misrepresentation;
- Identifying information, including the organizational affiliation in the Subscriber's certificate, changes before the certificate expires;
- The certificate subject can be shown to have violated the requirements of this CPS or the Subscriber agreement;
- The private key is suspected of compromise;
- The continued use of the certificate is harmful to the VeriSign ECA.

Note: There are no privilege attributes contained in VeriSign ECA certificates. 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 subsequent CRLs issued after they expire. A revoked certificate will appear on at least one CRL.

4.4.1.2 Who Can Request Revocation

The Subscriber is authorized to request the revocation of his or her own certificate. The VeriSign ECA RA, a Company RA, the Subscriber's authorizing organization, or a Trusted Agent can request the revocation of a Subscriber's certificate on the Subscriber's behalf. A Trusted Agent can only request revocation of a certificate for a Subscriber that is affiliated with the Trusted Agent's organization. Written notice including a reason for the revocation is also provided to a Subscriber whose certificate has been revoked.

4.4.1.3 Procedure for Revocation Request

The revocation request must identify the certificate to be revoked and must include the reason for revocation. The revocation requests may be manually or digitally signed and must be authenticated by a RA. The processes for revocation are as follows:

Certificate Revocation Request by Subscriber: An ECA Subscriber may request revocation of a certificate by sending a digitally signed message to the VeriSign ECA. The message must include at least one of the reasons for the revocation listed in Section 4.4.1.1. The VeriSign ECA RA will validate the request by verifying the signature on the signed message. If the Subscriber is not in possession of their private Identity key, he or she may also request revocation of his or her certificate by presenting the unique challenge password selected during certificate enrollment to a revocation Web page hosted by VeriSign. The Web page is protected using SSL. Upon successful validation of the revocation request by the ECA RA, the ECA RA submits the revocation request and the VeriSign ECA will change the certificate status in the repository from valid to revoked and the serial number of the revoked certificate will be placed on the next published CRL.

Certificate Revocation Request by Trusted Agent: A Trusted Agent may request revocation of a Subscriber's certificate by sending a digitally signed message to the VeriSign ECA RA. The Trusted Agent shall authenticate the Subscriber's request for revocation by validating the Subscriber's signature on a digitally signed-e-mail, by validating the Subscriber's identity in person, or by consulting an appropriate entity in the Subscriber's organization. The VeriSign ECA RA will validate the request by verifying the signature on the signed message and confirming that the Trusted Agent affiliation is the same as the affiliation in the Subscriber certificate(s) to be revoked. The message must identify the name and e-mail address of the Subscriber whose certificate(s) is to be revoked and the reason for the revocation. Upon successful validation of the revocation request by the VeriSign ECA RA, the ECA RA submits the revocation request and VeriSign ECA will change the certificate status in the Repository from valid to revoked and the serial number of the revoked certificate will be placed on the next published CRL.

Certificate Revocation Request by Company RA: A Company RA may request revocation of any ECA Subscriber certificate affiliated with their company/organization. The Company RA shall authenticate a Subscriber's request for revocation by validating the Subscriber's signature on a digitally signed-e-mail, by validating the Subscriber's identity in person, or by consulting an appropriate entity in the Subscriber's organization. Access to the VeriSign ECA to request revocation is protected using SSL and requires presentation of a valid RA certificate. The VeriSign ECA validates the RA certificate and checks that the RA affiliation is the same as the organizational affiliation in the certificate to be revoked. If these checks are successful, the VeriSign RA submits the request for revocation to the VeriSign ECA which will revoke the certificate and change the certificate status in the Repository from valid to revoked.

At least once every eighteen (18) hours, the VeriSign ECA will aggregate all unexpired 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 ECA revoke his or her certificate as soon as possible after the need for revocation has been determined. There is no grace period for the revocation of the certificate by the ECA.

4.4.2 Suspension

The VeriSign ECA platform does support certificate suspension. However, procedural controls are used to ensure that the VeriSign RA does not suspend an ECA certificate.

4.4.3 Certificate Revocation Lists

4.4.3.1 CRL Issuance Frequency

The VeriSign ECA will generate and issue CRLs at least every eighteen (18) hours. All CRLs shall have an eighteen (18) hour validity interval. Superseded CRLs are removed from the repository upon posting of the latest CRL. Revoked certificates are removed from the CRL after they have expired.

4.4.3.2 CRL Checking Requirements

The VeriSign ECA publishes information on how to obtain information on revoked certificates and will advise relying parties via a Relying Party Agreement on the need to check certificate revocation status. If a Relying party is unable to obtain revocation information for an ECA certificate, the Relying party must either reject use of the certificate, or make an informed decision to accept the risk, responsibility, and consequences of using certificate whose authenticity cannot be guaranteed.

4.4.4 Online Status Checking

VeriSign will provide an online CSA to enable certificate status checking using the Online Certificate Status Protocol (OCSP). Separate OCSP responders will be provided for status checking of ECA client and ECA server certificates. Each OCSP responder will be issued a medium hardware assurance certificate in the format specified in Appendix A. The OCSP certificates will be signed by the appropriate VeriSign ECA Client or Server Subordinate CA. The OCSP responders shall ensure that accurate and up-to-date certificate status information is provided in the revocation status response and shall digitally sign all responses.

4.4.5 Other Forms of Revocation Advertisements Available

The VeriSign ECA will also provide an SSL-protected Web page at which relying parties may query the revocation state of a Subscriber certificate. This Web page is located at https://eca.verisign.com.

4.4.6 Special Requirements Related to Key Compromise

VeriSign ECA CMAs shall have the capability to transition any revocation reason code to compromise by logging on in an SSL client-authenticated session to the ECA RA administrator interface and authenticating with an RA administrator certificate stored on a FIPS 140-1/2 level 2 hardware cryptographic token. Access control for ECA RAs is based on the name, e-mail address, organization and department listed in the ECA RA administrator certificate issued by a separate VeriSign Administrator CA.

4.5 SECURITY AUDIT PROCEDURES

4.5.1 Types of Events Recorded

VeriSign will record events for the CA, RA, Company RAs and the CSA. The events include 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 audit data is recorded in a logbook, paper form, or other physical mechanism as appropriate to the process being audited.

4.6 RECORDS ARCHIVAL

4.6.1 Types of Data Archived

- The VeriSign ECA archive process records all relevant information, in either paper or electronic record format

4.6.2 Retention Period for Archive

VeriSign ECA archive records, including certificates, CRLs and ECA public keys, are retained for a period of at least ten (10) years and six (6) months. Prior to the end of the archive retention period, or a longer period agreed to by VeriSign and the EPMA, the VeriSign ECA shall transfer the archived data to an EPMA approved archival facility.

4.7 KEY CHANGEOVER

The ECA 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 6 years to ensure that the validity interval of user certificates (up to 3 years), will expire before the validity interval of the CA certificate. The ECA will change its keys every 3 years to ensure that no certificate is issued with a life beyond the expiration date of the CA certificate. The CA name will change with each key changeover. The old ECA CA keys will be retained to issue CRLs for Subscribers that have been issued certificates signed with the old ECA CA signing key.

4.8 COMPROMISE AND DISASTER RECOVERY

4.8.1 Compromise recovery

The VeriSign ECA will immediately notify the ECA Root CA and the EPMA in the event of a disaster or compromise. The ECA Root CA in turn will assist in communicating the revocation of the ECA certificate to all relying parties by publishing a CRL.

Upon issuance of a new VeriSign ECA certificate signed by the ECA Root, the VeriSign ECA will reconstitute its PKI operation using the same procedures that were performed during initial system initialization. All ECA Subscribers, RAs, Company RAs and TAs will be rekeyed using the same procedures used for initial certificate enrollment.

In the event of the compromise of the VeriSign ECA OCSP responder, the VeriSign ECA shall

revoke the OCSP responder certificate, add the certificate serial number to a CRL and subsequently re-key the OCSP responder.

In the event of the compromise of a RA or TA, the certificate of the compromised entity will be revoked and the RA or TA will be rekeyed using the same procedures used for initial certificate enrollment.

4.8.2 Disaster Recovery

VeriSign has developed a Disaster Recovery Plan for all of its managed PKI services including the ECA. The Disaster Recovery Plan defines the procedures for the VeriSign Disaster Recovery Team to reconstitute VeriSign ECA operations using backup data and backup copies of the ECA keys at the disaster recovery facility.

4.9 CA TERMINATION

In the event that the VeriSign ECA is terminated for the convenience of the EPMA, contract expiration, re-organization, or other non-security related reason, and provisions are made for the continuation of ECA revocation operations, the ECA certificate and all certificates issued by the VeriSign ECA will continue to be considered valid until their expiration. Otherwise, the VeriSign ECA shall revoke all certificates and issue a final CRL.

Upon direction of the EPMA, VeriSign will revoke the all Subscriber certificates and destroy all ECA private keys.

The ECA shall transfer its archival records to an EPMA approved archival facility

5. PHYSICAL, PROCEDURAL AND PERSONNEL SECURITY CONTROLS

5.1 PHYSICAL CONTROLS

The VeriSign ECA equipment is dedicated to the ECA function and does not perform non-CA related functions. The VeriSign ECA equipment includes, but is not limited to, the system running the ECA software, ECA hardware cryptographic module, and databases and directories located on ECA equipment. Databases and directories located on the ECA computer are not accessible to Subscribers or Relying Parties.

Unauthorized use of CMA equipment is forbidden. Physical security controls are implemented to protect the CMA hardware and software from unauthorized use. CMA cryptographic modules are protected against theft, loss and unauthorized use.

5.2 PROCEDURAL CONTROLS

5.2.1 Trusted Roles

All employees, contractors, and consultants of the VeriSign ECA 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. All employees serving in a trusted position must acquire and periodically re-qualify (every five years) for “trusted employee” status, as defined in section 5.3.2, as a condition of employment.

5.2.1.5 Trusted Agent

A *Trusted Agent* is a person authorized to act as a representative of the ECA RA in providing Subscriber identity verification during the registration process. Trusted Agents do not have automated interfaces with VeriSign ECAs. Trusted Agents are representatives of an organization that has entered into a contract with VeriSign for the volume purchase of ECA certificates.

5.2.1.6 PKI Sponsor

A *PKI Sponsor* fills the role of a Subscriber for non-human system components and organizations that are named as public key certificate subjects. The PKI Sponsor works with the VeriSign ECA RA and, when appropriate, Trusted Agents, to register components (web servers, routers, firewalls, etc.) in accordance with Section 3.1.10, and is responsible for meeting the obligations of Subscribers as defined throughout this document.

5.2.2 Separation of Roles

The VeriSign ECA maintains a policy and rigorous control procedures to ensure segregation of duties based on job responsibilities. No one person is assigned more than one of the roles defined in Section 5.2.1. The most sensitive tasks, such as access to and management of Cryptographic Signing Units (CSU) and associated key material, require multiple trusted employees. Operations performed by persons with root access require two persons to observe all activities. Access to root is from individual accounts and audited.

5.3 PERSONNEL SECURITY CONTROLS

5.3.1 Background, Qualifications, Experience and Clearance Requirements

All persons with unattended access to the VeriSign ECA and Repository are expressly approved and must be of unquestionable loyalty to the United States, trustworthiness, and integrity. All CMAs shall be US citizens.

The VeriSign ECA 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.

Personnel appointed to operate CMA equipment shall:

- Have successfully completed an appropriate training course;
- Have demonstrated the ability to perform their duties;
- Be trustworthy;
- Have no other duties that would interfere with their duties as a CMA;
- Have not been previously relieved of CMA or other trusted duties for reasons of negligence or non-performance of duties;
- Have not been denied a security clearance, or had a security clearance revoked;
- Have not been convicted of a felony offense; and
- Be appointed in writing by an approving authority, or be a party to a contract for PKI services

5.3.2 Background Check Procedures

a) All VeriSign persons filling trusted roles shall undergo a background investigation and a periodic reinvestigation. The scope of the background investigation is similar to the DOD Industrial Secret criteria.

5.3.3 Training Requirements

VeriSign Operations personnel are sufficiently trained prior to performing independent, unattended

duties.

Company RAs and TAs are trained using on-line web seminars and are provided with manuals defining their roles, obligations and required operational and security procedures and the requirements of the CP and CPS.

A training log is retained of each student who successfully completes a training (or retraining) module indicating the student trained, the training received, and the date the training was completed.

5.3.4 Retraining Frequency and Requirements

Personnel filling ECA PKI roles shall be aware of changes in the ECA operation. Any significant change to the ECA operations shall have a training plan and the execution of such plan shall be documented.

5.3.5 Job Rotation Frequency and Sequence

VeriSign shall manage job rotation frequency and sequence to provide continuity and integrity of the ECA service.

5.3.6 Sanctions for Unauthorized Actions

VeriSign ECA 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. VeriSign personnel who violate the provisions of this CPS are subject to administrative and disciplinary action, including suspension or termination.

5.3.7 Contracting Personnel Requirements

Any VeriSign ECA 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 including this CPS, VeriSign's security policy, system documents and role-specific training materials necessary 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. At no time does any entity's private key appear outside of the modules in which they are generated unless encrypted for local transmission or for processing or storage by a key recovery mechanism. Subscriber key pairs for Identity certificates are generated on the Subscriber's local system, and Subscriber key pairs for Encryption certificates are generated in FIPS 140-1/2 Level 2 hardware cryptographic tokens at the VeriSign Key Management System.

6.1.2 Private Key Delivery to Subscriber

See paragraph 4.2.1.

6.1.3 Key Sizes

All certificate signing key pairs and Subscriber key pairs will be 1024-bit RSA key pairs. Any use of Secure Socket Layer (SSL) protocol to accomplish the requirements of this CPS shall require 1024-bit RSA, SHA-1 and three key triple-Data Encryption Standard (triple-DES) for the symmetric key algorithm.

6.1.4 Public Key Parameters

Prime numbers for use with the RSA algorithm defined in [PKCS-1] shall be generated and checked in accordance with [PKCS-1].

6.1.5 Parameter Quality Checking

See Section 6.1.4.

6.1.6 Hardware/Software Key Generation

For medium hardware assurance, the Identity key pair is generated on the hardware token and the Encryption key pair is generated in a Key Management Server. After the Encryption key pair is downloaded to the hardware token, the key pair is erased in the Key Management Server and no copy, other than the authorized key escrow copy is retained. All key and pseudo-random number generation is performed using a FIPS approved method.

6.1.7 Key Usage Purposes

The VeriSign ECA shall issue Identity certificates with the key usage extension for signing and Encryption certificates with the key usage extension for encryption. Only VeriSign ECA SSL Web Server certificates shall have dual usage. All VeriSign ECA certificates shall meet the certificate profiles defined in Appendix A.

6.2 PRIVATE KEY PROTECTION

6.2.1 Standards for cryptographic modules

VeriSign ECA Subscribers are obligated to use cryptographic modules that meet at least the criteria for FIPS 140-1/2 Level 1. No one shall have access to a private signing key but the Subscriber. The VeriSign ECA RA and Company RAs use FIPS 140-1/2 Level 2 certified hardware cryptographic tokens, and the VeriSign ECA CA and CSA use FIPS 140-1/2 Level 3 hardware cryptographic tokens.

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

Any private Encryption keys held by a CMA shall be held in strictest confidence and controlled as described in the ECA Key Recovery Policy (KRP) and the VeriSign ECA Key Recovery Practice Statement (KRPS).

Note that Section 6.1.1 stipulates cryptographic module requirements for key generation.

6.2.2 Private Key Multi-person Control

Both the operational and backup versions of the VeriSign ECA private key are subject to multi-person control over activation of the hardware cryptographic device containing the private key. A list identifying the parties responsible for this control will be made available for inspection during compliance audits.

6.2.3 Private Key Escrow

The VeriSign ECA provides key escrow and a key recovery service for VeriSign ECA Subscriber private Encryption keys. Private keys used to support non-repudiation services are never escrowed. The method, procedures and controls which apply to the storage, request for, extraction and/or retrieval, delivery, protections and destruction of the requested copy of an escrowed ECA Subscriber private Encryption key are described in the VeriSign ECA Key Recovery Practice Statement (KRPS).

6.2.4 Private Key backup

VeriSign ECA Subscribers are obligated to take precautions necessary 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. The VeriSign ECA provides escrow of Subscriber private Encryption keys, but Subscriber private Identity keys are never escrowed.

6.2.5 Private Key Archival

See Section 6.2.3 and Section 6.2.4

6.2.6 Private Key entry into cryptographic module

When the VeriSign ECA 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 plaintext form outside the hardware protection boundary. Private keys for RAs are generated by and in a FIPS 140-1/2 Level 2 cryptographic module. RA private keys never exist in plain text form outside of the boundary of the

cryptographic module.
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 ECA and CSA hardware cryptographic devices utilize a multi-party activation mechanism. This activation data is generated during initialization of the device and split into shares stored on hardware tokens.

VeriSign ECA Subscribers and RAs 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 ECA become aware of the Subscriber's password. Similarly, the RA is the only entity that knows the password for the RA hardware token.

6.2.8 Method of Deactivating Private Key

Software cryptographic modules are deactivated upon session termination or log out from the workstation.

RA, CA, CSA and Subscriber tokens will deactivate their private keys upon removal from their readers. When not in use, the CA and CSA tokens are stored in a vault.

6.2.9 Method of Destroying Private Key

In the event the VeriSign ECA or CSA key requires destruction, the hardware token's "zeroize" command will be performed to do so. In the event the RA or Subscriber key requires destruction, the hardware token "initialize" command is used to zeroize the private key. For software cryptographic modules, this can be by overwriting the data.

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

The key usage periods for keying material is described in Section 3.2 and Section 4.7

6.4 ACTIVATION DATA

6.4.1 Activation data generation and installation

VeriSign ECA Subscribers are requested to select their own password to protect their private key. Guidance regarding the selection of a PIN in accordance with FIPS is provided during the enrollment process.

The activation data used to protect the VeriSign ECA and CSA hardware cryptographic devices is

randomly and automatically generated. Activation data protecting access to the ECA and CSA hardware cryptographic device is generated within a FIPS 140-1/2 Level 3 certified cryptographic module. RAs are also required to choose PINs in accordance with FIPS 112. RA PINs are required to be changed every 90 days.

The RA activation PIN is only known by the holder of the RA token.

6.4.3 Other aspects of activation data

See Section 6.4.1

6.5 COMPUTER SECURITY CONTROLS

6.5.1 Specific computer security technical requirements

The VeriSign ECA and CSA employ an operating system that has been selected by VeriSign for security functionality, including audit requirements, identification and authentication, and discretionary access controls.

6.5.2 Computer security rating

VeriSign uses Sun Microsystems's Solaris 2.8 operating system for production services. Earlier versions of Solaris (2.5.1 and 2.6) have been evaluated under the U.K. ITSEC program. Solaris 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.

6.6 LIFE CYCLE TECHNICAL CONTROLS

Equipment (hardware and software) procured to operate the VeriSign CA, RA and CSA is purchased in a fashion to reduce the likelihood that any particular component was tampered with, such as random selection. Intended use of any such procured hardware and software is never indicated on order forms/paperwork. All software received from vendors will be inspected for evidence of tampering. Only commercial software is required for Company RA workstations. Companies are advised that RA workstations and associated commercial software should be procured without indicating the intended use.

6.7 NETWORK SECURITY CONTROLS

The VeriSign ECA, RA and CSA are designed to mitigate risk to external threats.
Company RAs shall utilize a commercial-grade firewall in accordance with best industry practices and commercial virus scanning software (such as McAfee and Norton Anti-Virus)

6.8 CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

See Section 6.2.

7. CERTIFICATE AND CRL PROFILES

Appendix A contains the formats for the various certificates and CRLs.

7.1 CERTIFICATE PROFILE

7.1.1 Version Numbers

ECA shall issue X.509 Version 3 certificates only.

7.1.2 Certificate Extensions

The VeriSign ECA uses the certificate profiles as described in this CPS. These profiles are based on the *Federal PKI Certificate and CRL Profile* [FPKI-E].

7.1.3 Algorithm Object Identifiers

Certificates under this CPS will use the following OIDs for signatures.

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

Certificates under this CPS will use the following OIDs for identifying the algorithm for which the subject key was generated.

rsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}
dhpublicnumber	{iso(1) member-body(2) us(840) ansi-x942(10046) number-type(2) 1}
id-keyExchangeAlgorithm	{joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101) dod(2) infosec(1) algorithms(1) 22}

The VeriSign ECA shall certify only public keys associated with the crypto-algorithms identified above, and shall only use the signature crypto-algorithms described above to sign certificates, certificate revocation lists and any other PKI product, including other forms of revocation such as OCSP responses..

7.1.4 Name Forms

The subject and issuer fields of ECA certificates are populated with X.500 Distinguished Names. See Appendix A.

7.1.5 Name Constraints

The VeriSign ECA does not enforce name constraints.

7.1.6 Certificate Policy Object Identifier

Certificates issued by the VeriSign ECA shall assert the OID appropriate to the level of assurance with which it was issued as defined in Section 1.2.

7.1.7 Usage of Policy Constraints

The VeriSign ECA does not populate policy constraints.

7.1.8 Policy Qualifiers Syntax and Semantics

Certificates issued by the VeriSign ECA shall contain a URL pointer to a relying party agreement.

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

The ECA will not mark the certificate Policies as critical.

7.2 CRL PROFILE

7.2.1 Version numbers

CRLs issued under this CPS will be version 2 CRLs. The VeriSign ECA will not issue Authority Revocation Lists (ARLs) or any other partitioned CRLs.

7.2.2 CRL and CRL Entry Extensions

Detailed CRL profiles covering the use of each extension are available and described in Appendix A.

7.3 OCSP REQUEST-RESPONSE FORMAT

The VeriSign ECA supports pre-computed OCSP responses (i.e. no nonce) and the formats for OCSP request and response are compliant with RFC 2560.

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.

Prior to enactment, the EPMA must approve amendments to this CPS.

8.2 PUBLICATION AND NOTIFICATION PROCEDURES

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

This VeriSign ECA CPS is posted in the VeriSign document repository at http://www.verisign.com/repository/cps/. Applicable updates to the ECA CPS that affect Subscribers and relying parties will be posted on the VeriSign ECA home page.

8.3 CPS APPROVAL PROCEDURES

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

8.4 CPS WAIVERS

The EPMA is the final approval authority of any proposed waiver to the ECA CP which with this CPS is compliant.

APPENDIX A: CERTIFICATE AND CRL PROFILES

A.1 ECA ROOT CA SELF-SIGNED CERTIFICATE

Field	**ECA Root CA Value**
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Issuer Distinguished Name	cn=ECA Root CA, ou=ECA, o=U.S. Government, c=US
Validity Period	36 years from date of issue in Generalized Time format
Subject Distinguished Name	cn=ECA Root CA, ou=ECA, o=U.S. Government, c=US
Subject Public Key Information	1024 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Issuer Unique Identifier	Not Present
Subject Unique Identifier	Not Present
Issuer's Signature	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Extensions	
Authority key identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of the ECA Root CA's public key information)
subject key identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of the ECA Root CA's public key information)
key usage	c=yes; digitalSignature, keyCertSign, cRLSign
Extended key usage	Not Present
Private key usage period	Not Present
Certificate policies	c=no; {2 16 840 1 101 3 2 1 12 1}, {2 16 840 1 101 3 2 1 12 2}
Policy Mapping	Not Present
subject Alternative Name	Not Present
Issuer Alternative Name	Not Present
Subject Directory Attributes	Not Present
Basic Constraints	c=yes; cA=True; no path length constraint
Name Constraints	Not Present
Policy Constraints	Not Present
CRL Distribution Points	Not Present

A.2 SUBORDINATE CA – CLIENT CERTIFICATE ISSUER

Field	Subordinate CA Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Issuer Distinguished Name	cn=ECA Root CA, ou=ECA, o=U.S. Government, c=US
Validity Period	6 years from date of issue in UTCT format
Subject Distinguished Name	cn=VeriSign Client External Certification Authority, ou=Certification Authorities, ou=ECA, o=U.S. Government, c=US
Subject Public Key Information	1024 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Issuer Unique Identifier	Not Present
Subject Unique Identifier	Not Present
Issuer's Signature	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Extensions	
Authority key identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of the ECA Root CA's public key information)
subject key identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of the ECA public key information)
key usage	c=yes; digitalSignature, keyCertSign, cRLSign
Extended key usage	Not Present
Private key usage period	Not Present
Certificate policies	c=no; policyOID = {2 16 840 1 101 3 2 1 12 1}, {2 16 840 1 101 3 2 1 12 2}; cpsURI = https://www.verisign.com/repository/eca/cps
Policy Mapping	Not Present
subject Alternative Name	c=no; always present, contains directoryName
Issuer Alternative Name	Not Present
Subject Directory Attributes	Not Present
Basic Constraints	c=yes; cA=True; path length = 0
Name Constraints	c=no; permitted subtrees: ou=VeriSign, Inc., ou=ECA, o=U.S. Government, c=US
Policy Constraints	Not Present
Authority Information Access	Not Present
CRL Distribution Points	c = no; URI=ldap://ds-3.c3pki.chamb.disa.mil/cn%3dECA%20Root%20CA%2cou%3dECA%2co%3dU.S.%20Government%2cc%3dUS?certificaterevocationlist;binary

A.3 SUBORDINATE CA – COMPONENT CERTIFICATE ISSUER

Field	Subordinate CA Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Issuer Distinguished Name	cn=ECA Root CA, ou=ECA, o=U.S. Government, c=US
Validity Period	6 years from date of issue in UTCT format
Subject Distinguished Name	cn=VeriSign Server External Certification Authority, ou=Certification Authorities, ou=ECA, o=U.S. Government, c=US
Subject Public Key Information	1024 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Issuer Unique Identifier	Not Present
Subject Unique Identifier	Not Present
Issuer's Signature	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Extensions	
Authority key identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of the ECA Root CA's public key information)
subject key identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of the ECA public key information)
key usage	c=yes; digitalSignature, keyCertSign, cRLSign
Extended key usage	Not Present
Private key usage period	Not Present
Certificate policies	c=no; policyOID = {2 16 840 1 101 3 2 1 12 1}, {2 16 840 1 101 3 2 1 12 2}; cpsURI = https://www.verisign.com/repository/eca/cps
Policy Mapping	Not Present
subject Alternative Name	c=no; always present, contains directoryName
Issuer Alternative Name	Not Present
Subject Directory Attributes	Not Present
Basic Constraints	c=yes; cA=True; path length = 0
Name Constraints	c=no; permitted subtrees: ou=VeriSign, Inc., ou=ECA, o=U.S. Government, c=US
Policy Constraints	Not Present
Authority Information Access	Not Present
CRL Distribution Points	c = no; URI=ldap://ds-3.c3pki.chamb.disa.mil/cn%3dECA%20Root%20CA%2cou%3dECA%2co%3dU.S.%20Government%2cc%3dUS?certificaterevocationlist;binary

A.4 IDENTITY CERTIFICATE

Field	Identity Certificate Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-1WithRSAEncryption
Issuer Distinguished Name	cn=VeriSign Client External Certification Authority, ou=Certification Authorities, ou=ECA, o=U.S. Government, c=US
Validity Period	3 years from date of issue
Subject Distinguished Name	cn=<Subscriber Name>, ou=<Subscriber Company Name >, ou=VeriSign, Inc., ou=ECA, o=U.S. Government, c=US
Subject Public Key Information	1024 bit RSA key modulus, rsaEncryption
Issuer Unique Identifier	Not Present
Subject Unique Identifier	Not Present
Issuer's Signature	sha-1WithRSAEncryption
authority key identifier	c=no; octet string
subject key identifier	c=no; octet string
key usage	c=yes;digitalSignature, nonRepudiation
Extended key usage	Not Present
Private key usage period	Not Present
Certificate policies	c=no; policyOID = {2 16 840 1 101 3 2 1 12 1}; cpsURI = https://www.verisign.com/repository/eca/cps
Policy Mapping	Not Present
subject Alternative Name	c=no; always present, contains RFC822 email address
Issuer Alternative Name	Not Present
Subject Directory Attributes[4]	c=no; {id-pda-countryOfCitizenship AttributeType ::= {1 3 6 1 5 5 7 9 4 }[4] CountryOfCitizenship ::= PrintableString (SIZE (2) -- ISO 3166 Country Code}
Basic Constraints	Not Present
Name Constraints	Not Present
Policy Constraints	Not Present
Authority Information Access	c=no; accessMethod=caIssuers, accessLocation= https://eca.verisign.com/CA/VeriSignECA.cer accessMethod=OCSP, accessLocation= http://eca-client-ocsp.verisign.com
CRL Distribution Points	c = no; Full Name URI= http://eca-client-crl.verisign.com/VeriSignECA/LatestCRL.crl

[4] The system shall be capable of asserting multiple citizenships using the CountryOfCitizenship OID multiple times.

A.5 ENCRYPTION CERTIFICATE

Field	Encryption Certificate Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-1WithRSAEncryption
Issuer Distinguished Name	cn= VeriSign Client External Certification Authority, ou=Certification Authorities, ou=ECA, o=U.S. Government, c=US
Validity Period	3 years from date of issue
Subject Distinguished Name	cn=<Subscriber Name>, ou=<Subscriber Company Name >, ou=VeriSign, Inc., ou=ECA, o=U.S. Government, c=US
Subject Public Key Information	1024 bit RSA key modulus, rsaEncryption
Issuer Unique Identifier	Not Present
Subject Unique Identifier	Not Present
Issuer's Signature	sha-1WithRSAEncryption
authority key identifier	c=no; octet string
subject key identifier	c=no; octet string
key usage	c=yes; keyEncipherment
Extended key usage	Not Present
Private key usage period	Not Present
Certificate policies	c=no; policyOID = {2 16 840 1 101 3 2 1 12 1}; cpsURI = https://www.verisign.com/repository/eca/cps
Policy Mapping	Not Present
subject Alternative Name	c=no; always present, contains RFC822 email address
Issuer Alternative Name	Not Present
Subject Directory Attributes[5]	c=no; {id-pda-countryOfCitizenship AttributeType ::= {1 3 6 1 5 5 7 9 4 }[5] CountryOfCitizenship ::= PrintableString (SIZE (2) -- ISO 3166 Country Code}
Basic Constraints	Not Present
Name Constraints	Not Present
Policy Constraints	Not Present
Authority Information Access	c=no; accessMethod=caIssuers, accessLocation= https://eca.verisign.com/CA/VeriSignECA.cer accessMethod=OCSP, accessLocation= http://eca-client-ocsp.verisign.com
CRL Distribution Points	c = no; Full Name URI= http://eca-client-crl.verisign.com/VeriSignECA/LatestCRL.crl

[5] The system shall be capable of asserting multiple citizenships using the CountryOfCitizenship OID multiple times.

A.6 COMPONENT CERTIFICATE

Field	Component & Web Server Certificate Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-1WithRSAEncryption
Issuer Distinguished Name	cn= VeriSign Server External Certification Authority, ou=Certification Authorities, ou=ECA, o=U.S. Government, c=US
Validity Period	3 years from date of issue
Subject Distinguished Name	cn=<Host URL | IP Address | Host Name>, l=< Host Company Locality>, s=< Host Company State>, ou=VeriSign, Inc., ou=ECA, ou=<Host Company Name>, o=U.S. Government, c=US
Subject Public Key Information	1024 bit RSA key modulus, rsaEncryption
Issuer Unique Identifier	Not Present
Subject Unique Identifier	Not Present
Issuer's Signature	sha-1WithRSAEncryption
authority key identifier	c=no; octet string
subject key identifier	c=no; octet string
key usage	c=yes; keyEncipherment, digitalSignature
Extended key usage	Not Present
Private key usage period	Not Present
Certificate policies	c=no; policyOID = {2 16 840 1 101 3 2 1 12 1}; cpsURI = https://www.verisign.com/repository/eca/cps
Policy Mapping	Not Present
subject Alternative Name	c=no; always present, Host URL | IP Address | Host Name
Issuer Alternative Name	Not Present
Subject Directory Attributes	Not Present
Basic Constraints	Not Present
Name Constraints	Not Present
Policy Constraints	Not Present
Authority Information Access	c=no; accessMethod=caIssuers, accessLocation= https://eca.verisign.com/CA/VeriSignECASSL.cer accessMethod=OCSP, accessLocation= http://eca-server-ocsp.verisign.com
CRL Distribution Points	c = no; Full Name URI=http://eca-server-crl.verisign.com/VeriSignECA/LatestCRL.crl

A.7 OCSP RESPONDER CERTIFICATE FOR CLIENT-ISSUING CA

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Issuer Distinguished Name	cn=VeriSign Client External Certification Authority, ou=Certification Authorities, ou=ECA, o=U.S. Government, c=US
Validity Period	One month from date of issue in UTCT format
Subject Distinguished Name	cn= VeriSign Client ECA OCSP Responder, ou=VeriSign, Inc., ou=ECA, o=U.S. Government, c=US
Subject Public Key Information	1024 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Issuer Unique Identifier	Not Present
Subject Unique Identifier	Not Present
Issuer's Signature	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Extensions	
Authority key identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of the ECA CA's public key information)
subject key identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of the OCSP Responder public key information)
key usage	c=yes; nonRepudiation, digitalSignature
Extended key usage	c=yes; id-kp-OCSPSigning {1 3 6 1 5 5 7 3 9}
Certificate policies	c=no; policyOID = {2 16 840 1 101 3 2 1 12 2}; cpsURI = https://www.verisign.com/repository/eca/cps
subject Alternative Name	c=no; always present, contains directoryName
No Check	id-pkix-ocsp-nocheck; {1 3 6 1 5 5 7 48 1 5}
Authority Information Access	c=no; accessMethod=caIssuers, accessLocation= https://eca.verisign.com/CA/VeriSignECA.cer

A.8 OCSP RESPONDER CERTIFICATE FOR COMPONENT-ISSUING CA

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Issuer Distinguished Name	cn=VeriSign Server External Certification Authority, ou=Certification Authorities, ou=ECA, o=U.S. Government, c=US
Validity Period	One month from date of issue in UTCT format
Subject Distinguished Name	cn= VeriSign Server ECA OCSP Responder, ou=VeriSign, Inc., ou=ECA, o=U.S. Government, c=US
Subject Public Key Information	1024 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Issuer Unique Identifier	Not Present
Subject Unique Identifier	Not Present
Issuer's Signature	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Extensions	
Authority key identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of the ECA CA's public key information)
subject key identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of the OCSP Responder public key information)
key usage	c=yes; nonRepudiation, digitalSignature
Extended key usage	c=yes; id-kp-OCSPSigning {1 3 6 1 5 5 7 3 9}
Certificate policies	c=no; policyOID = {2 16 840 1 101 3 2 1 12 2}; cpsURI = https://www.verisign.com/repository/eca/cps
subject Alternative Name	c=no; always present, contains directoryName
No Check	id-pkix-ocsp-nocheck; {1 3 6 1 5 5 7 48 1 5}
Authority Information Access	c=no; accessMethod=caIssuers, accessLocation= https://eca.verisign.com/CA/VeriSignECASSL.cer

A.9 SUBORDINATE CA CRL – FOR CLIENT-ISSUING CA

Field	Subordinate CA CRL Value
Version	V2 (1)
Issuer Signature Algorithm	sha-1WithRSAEncryption
Issuer Distinguished Name	cn=VeriSign Client External Certification Authority, ou=Certification Authorities, ou=ECA, o=U.S. Government, c=US
thisUpdate	UTCT
nextUpdate	UTCT; thisUpdate + 18 hours
Revoked certificates list	0 or more 2-tuple of certificate serial number and revocation date (in UTCT)
CRL extensions	
CRL Number	Integer
Authority Key Identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of the ECA public key information)
CRL entry extensions	
Invalidity Date	optional
Reason Code	Always Present; Will not include certificateHols

A.10 SUBORDINATE CA CRL – FOR COMPONENT-ISSUING CA

Field	Subordinate CA CRL Value
Version	V2 (1)
Issuer Signature Algorithm	sha-1WithRSAEncryption
Issuer Distinguished Name	cn=VeriSign Server External Certification Authority, ou=Certification Authorities, ou=ECA, o=U.S. Government, c=US
thisUpdate	UTCT
nextUpdate	UTCT; thisUpdate + 18 hours
Revoked certificates list	0 or more 2-tuple of certificate serial number and revocation date (in UTCT)
CRL extensions	
CRL Number	Integer
Authority Key Identifier	Octet String (20 byte SHA-1 hash of the binary DER encoding of the ECA public key information)
CRL entry extensions	
Invalidity Date	optional
Reason Code	Always Present; Will not include certificateHols

APPENDIX B: DEFINITIONS

access	Ability to make use of any information system (IS) resource. [NS4009]
access control	Process of granting access to information system resources only to authorized users, programs, processes, or other systems. [NS4009]
accreditation	Formal declaration by a Designated Approving Authority that an IS is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. [NS4009]
applicant	The Subscriber is sometimes also called an "applicant" after applying to a certification authority for a certificate, but before the certificate issuance procedure is completed. [ABADSG footnote 32]
archive	Long-term, physically separate storage.
Attribute Authority	An entity, recognized by a CMA, as having the authority to verify the association of attributes to an identity.
audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures. [NS4009]
audit data	Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event. [NS4009, "audit trail"]
authentication	Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information. [NS4009]
backup	Copy of files and programs made to facilitate recovery if necessary. [NS4009]
binding	Process of associating two related elements of information. [NS4009]
biometric	A physical or behavioral characteristic of a person.
Certificate Management Authority (CMA)	A Certification Authority or a Registration Authority.
Certificate Status Authority	A trusted entity that provides on-line verification to a Relying Party of a subject certificate's trustworthiness, and may also provide additional attribute information for the subject certificate.
Certification Authority (CA)	An authority trusted by one or more users to create and assign certificates. [ISO9594-8]
CA facility	The collection of equipment, personnel, procedures and structures that are used by a Certification Authority to perform certificate issuance and revocation.
certificate	A digital representation of information which at least (1) identifies the certification authority issuing it, (2) names or identifies its Subscriber, (3) contains the Subscriber's public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it. [ABADSG]
certificate-related information	Information, such as a Subscriber's postal address, that is not included in a certificate, but that may be used by a CA in certificate management.
challenge password	A secret chosen by a Subscriber during enrollment for a certificate. A CA or RA may use the challenge password to authenticate a Subscriber requesting revocation if the Subscriber is not able to prove possession of the private key.

client (application)	A system entity, usually a computer process acting on behalf of a human user that makes use of a service provided by a server.
Company RA	A person appointed by a company to perform RA functions on behalf of employees of the company or its affiliates.
compromise	Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred. [NS4009]
confidentiality	Assurance that information is not disclosed to unauthorized entities or processes. [NS4009]
cryptographic module	The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module. [FIPS1401]
cryptoperiod	Time span during which each key setting remains in effect. [NS4009]
dual use certificate	A certificate that is intended for use with both digital signature and data encryption services.
e-commerce	The use of network technology (especially the Internet) to buy or sell goods and services
Encryption (or Confidentiality) certificate	A certificate containing a public key that is used to encrypt or decrypt electronic messages, files, documents, or data transmissions, or to establish or exchange a session key for these same purposes. The process of storing protecting and escrowing the private component of the key pair associated with the encryption certificate is sometimes referred to as key management.
erroneous issuance	Issuance of a certificate not materially in accordance with the procedures required by the CPS, issuance of a certificate to a person other that 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.
External Policy Management Authority (EPMA)	Authority that oversees the creation and update of Certificate Policies, reviews Certification Practice Statements, reviews the results of CA audits for policy compliance, evaluates non-domain policies for acceptance within the domain, and generally oversees and manages the PKI certificate policies.
firewall	Gateway that limits access between networks in accordance with local security policy. [NS4009]
impersonation	Requesting and being issued a certificate issued under this CPS based on false or falsified information relating to naming or identity.
integrity	Protection against unauthorized modification or destruction of information. [NS4009]
intellectual property	Useful artistic, technical, and/or industrial information, knowledge or ideas that convey ownership and control of tangible or virtual usage and/or representation.
intermediate CA	A CA that is subordinate to another CA, and has a CA subordinate to itself.
key escrow	The retention of the private component of the key pair associated with a Subscriber's encryption certificate to support key recovery.
key exchange	The process of exchanging public keys (and other information) in order to establish secure communication.
key generation material	Random numbers, pseudo-random numbers, and cryptographic parameters used in generating cryptographic keys.
naming authority	An organizational entity responsible for assigning distinguished names (DNs) and for assuring that each DN is meaningful and unique within its domain.

non-repudiation	Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data. [NS4009]
Non-verified Subscriber Information	Information submitted by a Certificate Applicant to a CA or RA, and included within a Certificate, that has not been confirmed by the CA or RA and for which the applicable CA and RA provide no assurances other than that the information was submitted by the Certificate Applicant.
PKI Sponsor	Fills the role of a Subscriber for non-human system components or organizations that are named as public key certificate subjects, and is responsible for meeting the obligations of Subscribers as defined throughout this document.
privacy	State in which data and system access is restricted to the intended user community and target recipient(s).
Private key compromise	A loss, theft or 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.
Public Key Infrastructure (PKI)	Framework established to issue, maintain, and revoke public key certificates.
Registration Authority (RA)	Entity responsible for identification and authentication of certificate subjects that has automated equipment for the communication of applicant data to Certification Authorities and does not sign or directly revoke certificates.
Root CA	In a hierarchical PKI, the CA whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain.
re-key (a certificate)	To change the value of a cryptographic key that is being used in a cryptographic system application.
Relying Party	A person who has received a certificate and a digital signature verifiable with reference to a public key listed in the certificate, and is in a position to rely on them. [ABADSG]
renew (a certificate)	The act or process of extending the validity of the data binding asserted by a public key certificate by issuing a new certificate.
repository	A trustworthy system for storing and retrieving certificates or other information relevant to certificates. [ABADSG]
risk	An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.
risk tolerance	The level of risk an entity is willing to assume in order to achieve a potential desired result.
server	A system entity that provides a service in response to requests from clients.
signature or identity certificate	A public key certificate that contains a public key intended for verifying digital signatures rather than encrypting data or performing any other cryptographic functions.
subordinate CA	In a hierarchical PKI, a CA whose certificate signing key is certified by another CA, and whose activities are constrained by that other CA. (see superior CA)
Subscriber	An entity that (1) is the subject named or identified in a certificate issued to such an entity, and (2) holds a private key that corresponds to a public key listed in that certificate. [ABADSG]. **Current Subscribers** possess valid ECA-issued certificates.
superior CA	In a hierarchical PKI, a CA that has certified the certificate signing key of another CA, and that constrains the activities of that CA. (see subordinate CA)

system equipment configuration	A comprehensive accounting of all system hardware and software types and settings.
technical non-repudiation	The contribution public key mechanisms make to the provision of technical evidence supporting a non-repudiation security service.
threat	Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service. [NS4009]
tier	A physical barrier such as a locked door or closed gate or safe that provides mandatory access control and requires a positive response (e.g. door unlocks) before allowing access to the next area.
trust list	Collection of Trusted Certificates used by Relying Parties to authenticate other certificates.
Trusted Agent	Entity authorized to act as a representative of a Certificate Management Authority in providing Subscriber identification during the registration process. Trusted Agents do not have automated interfaces with Certification Authorities.
Trusted Certificate	A certificate that is trusted by the Relying Party on the basis of secure, authenticated delivery. The public keys included in Trusted Certificates are used to start certification paths. Also known as a "trust anchor".
Trusted Timestamp	A digitally signed assertion by a trusted authority that a specific digital object existed at a particular time.
two person control	Continuous surveillance and control of positive control material at all times by a minimum of two authorized individuals, each capable of detecting incorrect and/or unauthorized procedures with respect to the task being performed and each familiar with established security and safety requirements. [NS4009]
update (a certificate)	The act or process by which data items bound in an existing public key certificate, especially authorizations granted to the subject, are changed by issuing a new certificate.
unauthorized revocation	Revocation of a certificate without the authorization of the Subscriber.
zeroize	A method of erasing electronically stored data by altering the contents of the data storage so as to prevent the recovery of the data. [FIPS140]

APPENDIX C: IDENTITY PROOFING OUTSIDE THE U.S.

All identity proofing for U.S. citizens and non-U.S. citizens located outside the U.S. must be carried out in accordance with this Appendix C.

Identity proofing for U.S citizens and non-U.S. citizens located in the U.S. must be carried out in accordance with Section 3.1.9 of this CPS.

C.1 IDENTITY PROOFING BY U.S. CONSULAR OFFICERS

U.S. citizens located outside the U.S. can use the notarial services provided by U.S. consular offices and embassies for identity proofing purposes under this CPS. Non-U.S. citizens of those countries identified in Section C.1.3 below may also use these services for identity proofing when identity proofing is performed in one of these countries. Non-U.S. citizens who are not citizens of the countries identified in Section C.1.3 below must either comply with the requirements of Section C.2 to obtain their identity proofing, or they must be located in the U.S and must follow the procedures in Section 3.1.9 of this CPS.

C.1.1 Procedures for Identity Proofing by U.S. Consular Officers

Consular officers may act as notaries public for the purpose of performing identity proofing for ECA certificate applicants. Consular Officers at U.S. embassies and consulates abroad have the authority to administer to or take from any person any oath, affirmation, affidavit, or deposition, and to perform any other notarial act which any Notary Public is required or authorized by law to do within the United States. When identity proofing is performed by U.S. consular officers, all CPS requirements for identity proofing by notaries must be met. In addition, applicants must present a current valid passport for proof of citizenship as one of the documents proving identity.

Locations of U.S. consular offices and embassies may be found at:

- http://travel.state.gov/travel/tips/embassies/embassies_1214.html

C.1.2 ECA Requirements

In addition to meeting all other requirements of this CPS, including identity proofing using a notary, all certificates issued based on identity proofing performed by a U.S. consular officer must assert the country of citizenship of the applicant. The VeriSign ECA must verify that the documentation received contains the seal of a consular officer from one of the countries identified in Section C.1.3. The VeriSign ECA must also verify that the applicant presented a passport as one of the identity documents and for proof of citizenship.

C.1.3 Participating Countries

• Australia

• Canada

• New Zealand

• United Kingdom

C.2 IDENTITY PROOFING BY AUTHORIZED DOD EMPLOYEES

Authorized DOD employees who meet the requirements specified in the ECA CP may perform identity and citizenship verifications of individuals who do not reside in or are not citizens of the countries listed in Section C.1.3.

Identity proofing by authorized DOD employees is subject to compliance audit requirements as outlined in Section 2.7 of the ECA CP. Procedures followed by authorized DOD employees are subject to compliance audit only by the EPMA at the discretion of the DOD PKI ECA Liaison Officer.

C.2.1 Process for Authorizing Issuance of ECA Certificates When Identity Proofing Is Performed by Authorized DOD Employees Outside the U.S.

A DOD Component that desires to authorize employees to perform identity proofing outside the U.S. must complete the process defined in Section C.2.1 of the ECA CP.

The list of authorized DOD employees for each DOD Component, along with their certificate information, will be provided by the DOD PKI ECA Liaison Officer to the VeriSign ECA in a digitally signed email. The VeriSign ECA must validate the signature on the e-mail.

C.2.2 Identity Proofing Procedures to Be Used by Authorized DOD Employees for ECA Certificates

Authorized DOD employees must adhere to the following requirements for performing authentication of identity and citizenship of non-U.S. citizens applying for ECA certificates:

• The authorized DOD employee must know the country representative who provides the approved citizen list and verify that the country representative is on the list of approved country representatives.

• The authorized DOD employee must have a copy of the list of individuals of the country who are authorized to receive certificates, which shall include assertion of their citizenship. The authorized DOD employee must authenticate the list and may only accept it if the source is the DOD Component POC.

• The authorized DOD employee must be able to recognize passports for the country of citizenship of the applicant.

• The applicant and the country representative must appear together, in person, before the authorized DOD employee. The authorized DOD employee must verify that the applicant is on the list of individuals.

• Prior to appearing before the authorized DOD employee, the applicant must first enroll for a VeriSign ECA certificate, which creates a pending certificate request in the VeriSign ECA system. The Subscriber must print the VeriSign ECA Subscriber Enrollment Form and present it to the authorized DOD employee. The Subscriber Enrollment Form, which is populated with the identity and citizenship information entered online as part of the certificate enrollment process effectively binds the Subscriber identity to the certificate request because only the Subscriber possesses the private key associated with the pending certificate request.

• The applicant must present the Subscriber Enrollment Form and two forms of identification, at least one of which must be a passport, and both of which forms of identification must be recognized as legitimate identity documents by the authorized DOD employee.

• The applicant must sign a copy of the VeriSign ECA Subscriber Enrollment Form in the presence of the authorized DOD employee.

• The authorized DOD employee must examine the two forms of identification, record the type, identifying number and expiration date of each, and sign the VeriSign ECA Subscriber Enrollment Form. The authorized DOD employee must retain a copy and provide a copy of the signed form to the applicant. DOD Components may choose to maintain Subscriber Enrollment Forms in a centralized location, in which case the DOD Component PKI POC must provide the authorized DOD employees with instructions for transferring the forms to the centralized location.

• The authorized DOD employee must send an email to eca-trustedagent@verisign.com digitally signed with the employee's CAC signature certificate and containing the following information extracted from the Subscriber Enrollment Form:

- The name of the applicant,
- The organization of the applicant
- The e-mail address of the application
- The citizenship of the applicant asserted by the country representative

The e-mail must also include:

- A statement that the authorized DOD employee has performed identity proofing for this applicant in accordance with the ECA CP

C.2.3 ECA Requirements

In addition to meeting all other requirements of the ECA CP, the VeriSign ECA must adhere to the following requirements when accepting identity proofing performed by authorized DOD employees:

• Obtain in an authenticated manner the list of authorized DOD employees from the DOD PKI ECA Liaison Officer.

• Provide the email address (eca-trustedagent@verisign.com) that authorized DOD employees must use when sending to the VeriSign ECA the confirmation that identity proofing has taken place.

• Provide a copy of the VeriSign ECA Subscriber Agreement to all applicants.

• Receive, prior to each certificate issuance, an email digitally signed by a CAC-based signature certificate of the authorized DOD employee, asserting that the identity proofing has taken place. The ECA shall verify the signature on the email, including full certification path validation, as described in [RFC 3280]. The ECA shall also verify that the signer of the email is on the list of authorized DOD employees.

• Check the Subscriber data contained in the e-mail for consistency with the enrollment data previously entered online by the Subscriber (name, e-mail address, country of citizenship). After completion of these checks, the VeriSign RA approves the enrollment request, and an e-mail is sent to the Subscriber with two URLs, PINs and instructions for picking up the Identity and Encryption certificates.

• Assert the country of citizenship of the applicant for all certificates issued based on identity proofing performed by an authorized DOD employee.

C.2.4 Participating Countries

DOD Components may apply this identity proofing process in all countries and to qualified foreign nationals, except countries or entities or nationals proscribed by law and regulation at the time of application for certificate. Relevant laws and regulations include:

• Department of State International Traffic in Arms Regulations (ITAR) Proscribed List

(22 C.F.R. Section 126.1)

• Department of Commerce Export Administration Regulations (EAR), 15 C.F.R. Section 730 et seq., including specifically, but not limited to, Parts 736, 738, 740, 744 Spir, and 746. See http://www.access.gpo.gov/bis/ear/ear_data.html

• Department of the Treasury regulations issued pursuant to the International Emergency

Economic Powers Act (IEEPA), 50 U.S.C. Ch.35, Sec. 1701 et seq. or other laws identifying prohibited countries or people or entities, including the Office of Foreign Assets Control (OFAC) Listing of Specially Designated Nationals and Blocked Persons (SDN List) and OFAC Country Sanctions Programs.

APPENDIX D: REFERENCES

The following documents contain information that provides background, examples, or details about the contents of this policy.

Number	Title	Revision	Date
ABADSG	*Digital Signature Guidelines* http://www.abanet.org/scitech/ec/isc/dsgfree.html		1 August 1996
FIPS140	*Security Requirements for Cryptographic Modules* http://csrc.nist.gov/publications/index.html		21 May 2001
FIPS112	*Password Usage* http://csrc.nist.gov/		5 May 1985
FIPS186-2	*Digital Signature Standard* http://csrc.nist.gov/fips/fips186-2.pdf		20 January 2000
FOIAACT	*5 U.S.C. 552, Freedom of Information Act* http://www4.law.cornell.edu/uscode/5/552.html		
FPKI-Prof	*Federal PKI Certificate and CRL Extensions Profile* http://csrc.nist.gov/pki/		31 May 2002
NS4009	*NSTISSI 4009, National Information Systems Security Glossary*		January 1999
PKCS-1	*PKCS #1 v2.0: RSA Cryptography Standard* http://www.rsa.com		1 October 1998
PKCS-12	*Personal Information Exchange Syntax Standard* http://www.rsa.com/rsalabs/pubs/PKCS/html/pkcs-12.html		April 1997
ECAKRP	*Key Recovery Policy for External Certification Authorities*	Version 1.0	4 June 2002
RFC2527	*Certificate Policy and Certification Practices Framework*, Chokhani and Ford http://www.ietf.org/rfc/rfc2527.txt		March 1999

APPENDIX E: ACRONYMS AND ABBREVIATIONS

CA	Certification Authority
CMA	Certificate Management Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSA	Certificate Status Authority
CSOR	Computer Security Objects Registry
DES	Data Encryption Standard
DN	Distinguished Name
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
ECA	External Certification Authority
EPMA	ECA Policy Management Authority
FBCA	Federal Bridge Certification Authority
FIPS	Federal Information Processing Standard
FPKI	(US) Federal Public Key Infrastructure
I&A	Identification and Authentication
ID	Identity (also, a credential asserting an identity)
ISO	International Organization for Standards
KRP	Key Recovery Policy
KRPS	Key Recovery Practice Statement
LDAP	Lightweight Directory Access Protocol
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PIN	Personal Identification Number
PKCS	Public Key Certificate Standard
PKI	Public Key Infrastructure
RA	Registration Authority
RFC	Request For Comment
RSA	Rivest, Shamir, Adleman (encryption and digital signature algorithm)
S/MIME	Secure Multipurpose Internet Mail Extensions
SSL	Secure Socket Layer
USC	United States Code
USD	United States Dollar

APPENDIX F: VERISIGN ECA SUBSCRIBER AGREEMENT

External Certification Authority Subscriber Agreement

YOU MUST READ THIS EXTERNAL CERTIFICATION AUTHORITY SUBSCRIBER AGREEMENT ("SUBSCRIBER AGREEMENT") BEFORE APPLYING FOR, ACCEPTING, OR USING THE ECA ENCRYPTION AND ECA IDENTITY CERTIFICATE (COLLECTIVELY, "CERTIFICATE"). THIS AGREEMENT BECOMES EFFECTIVE WHEN YOU DOWNLOAD AND ACCEPT AN ECA CERTIFICATE.

This Subscriber Agreement details the terms and conditions regarding your application for a Certificate and, if VeriSign accepts your Certificate application, the terms and conditions regarding your use of the Certificate to be issued by VeriSign to you as a "Subscriber" of that Certificate. A Certificate is an electronic credential that uses public key cryptography. Each holder of a Certificate has a public/private key pair. The private key, which is held securely by the holder, is used for creating digital signatures. The public key, which may be widely distributed, is used to enable other users to verify digital signatures created by the holder of the private key. In order to rely on a public key, it is necessary that it be certified by an entity called a Certification Authority ("CA"). The CA binds a Subscriber's public key to his or her identity, certifies the public key and creates an electronic credential called the Certificate. The Certificate to be issued to you is part of the VeriSign External Certification Authority ("ECA") public key infrastructure in support of the ECA initiative of the United States Department of Defense ("DOD"). The Certificate is intended for use by entities such as US Government contractors and external organizations to enable secure, interoperable communications with the DOD, federal, state and local government agencies. Selected portions of the VeriSign ECA Certification Practice Statement ("CPS") and the VeriSign ECA Key Recovery Practice Statement ("KRPS"), as amended from time to time, are available publicly at VeriSign's website, www.verisign.com/repository.

Definitions.

The **ECA Identity Certificate** is used for authenticating the user and/or to verify the user's digital signature in electronic applications. There is just one (1) copy of the private key associated with the ECA Identity Certificate and it is controlled exclusively by you.

The **ECA Encryption Certificate** is intended to be used for encryption of communication and data. A copy of the private key associated with the ECA Encryption Certificate will be held securely in escrow with VeriSign. In the event that you lose access to the private key associated with your ECA Encryption Certificate, or if there is an authorized order to recover this private key, VeriSign will provide services to recover it. VeriSign will charge a fee, as set forth on VeriSign's website and updated from time to time, to recover the subscriber's ECA Encryption Certificate private key.

A **Registration Authority** ("RA") is a person or entity approved by VeriSign to authenticate Certificate applicants per the requirements in the VeriSign ECA CPS and to approve or reject Certificate, revoke Certificates, and renew Certificates.

A **Key Recovery Agent** ("KRA") is a person or entity approved by VeriSign to authenticate key recovery Requestors, per the requirements in the VeriSign ECA CPS and KRPS, and to approve or reject key recovery applications, and recover ECA Encryption Certificate private keys.

A **Requestor** means you or anyone authorized (e.g., supervisor, corporate officer, or law enforcement officer) to recover your ECA Encryption Certificate private key.

A **Trusted Agent** is a person appointed by a company or organization that is responsible for authenticating Subscribers, revocation requests, and Requestors per the requirements of the VeriSign ECA CPS and KRPS.

1. Certificate Application and Issuance. You must provide accurate information on your Certificate application. Upon completion of validation procedures required for your Certificate, VeriSign, an authorized Trusted Agent, or RA will process your Certificate application. VeriSign will notify you when your Certificate application is approved or rejected. If approved, VeriSign will issue you a Certificate for your use in accordance with this Subscriber Agreement. Some of the information you provide in your Certificate application will be contained in your Certificate and will be published in the VeriSign ECA repository. When you pick up your Certificate, you are deemed to have accepted the Certificate and agree to be bound to the terms of this Subscriber Agreement. You must review the information in your Certificate before using it and promptly notify VeriSign, the Trusted Agent, or RA of any errors. Upon receipt of such notice, VeriSign, the authorized Trusted Agent, or RA shall revoke your Certificate and issue a corrected Certificate. VeriSign has the right to refuse to issue a Certificate for any reason, in its sole discretion, without incurring any liability for any loss or expenses from such refusal. By accepting a Certificate, you acknowledge that you agree to the terms and conditions contained in the ECA CP, the VeriSign ECA CPS, and this Subscriber Agreement.

2. Subscriber Obligations and Use Limits. In addition to the terms of this Subscriber Agreement, you agree to use the private key and Certificate only in accordance with the VeriSign ECA Certificate Policy ("CP"), the VeriSign ECA Key Recovery Policy ("KRP"), and the VeriSign ECA CPS and VeriSign KRPS. Certificates issued within the ECA PKI are not designed, intended, or authorized for use as control equipment in hazardous circumstances or for uses requiring fail-safe performance such as the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control systems, or weapons control systems, where failure could lead directly to death, personal injury, or severe environmental damage. Therefore, you agree not to use your Certificate in any such situation.

3. Security Requirements and Revocation. You must protect your private key at all times in accordance with the VeriSign ECA CPS and this Subscriber Agreement. You must use a FIPS 140-1/2 Level 1or higher crypto module to generate and protect your private key. Your workstation must be protected using appropriate physical, procedural, operating system and boundary protection (e.g., firewall) security. In addition, you must not allow others to access your private key, crypto module, password, or any other security mechanisms protecting your private key. The private key of the ECA Encryption Certificate will be securely escrowed with VeriSign. If you know or suspect that a compromise of your private key has occurred, you must promptly notify VeriSign or, if applicable,

the Trusted Agent or RA and request that the Certificate be revoked. The Certificate will be revoked after your request is authenticated by VeriSign or, if applicable, the Trusted Agent or RA. You agree that VeriSign is entitled to investigate all actual or suspected compromises of your private key or breach in the security of the VeriSign ECA PKI as permitted by law and you must reasonably cooperate with VeriSign in any such investigation. You agree that VeriSign, an authorized Trusted Agent, or the RA is entitled to revoke your Certificate upon an actual or suspected compromise of your private key if you materially breach this Agreement (including not paying the required Certificate fee, if applicable), or if VeriSign, in it sole discretion, determines that your Certificate was issued in a manner that materially differed from what is required under the VeriSign ECA CPS and KRPS. You further agree that VeriSign is entitled to revoke your Certificate for other reasons, provided that VeriSign either: (i) promptly replaces your Certificate with a comparable Certificate; or (ii) provides reasonable compensation. Upon expiration or notice of revocation of your ECA Identity Certificate, you shall no longer use this certificate and the associated private key for any purpose and shall destroy the private key as specified in CPS section 6.2.9.

4. Ownership. Except as otherwise set forth herein, all right, title and interest in and to all VeriSign (i) registered and unregistered trademarks, service marks and logos; (ii) patents, patent applications, and patentable ideas, inventions, and/or improvements; (iii) trade secrets, proprietary information, and know-how; (iv) all divisions, continuations, reissues, renewals, and extensions thereof now existing or hereafter filed, issued, or acquired; (v) registered and unregistered copyrights including, without limitation, any forms, images, audiovisual displays, text, software; and (vi) all other intellectual property, proprietary rights or other rights related to intangible property which are used, developed, comprising, embodied in, or practiced in connection with any of the VeriSign services identified herein ("VeriSign Intellectual Property") are owned by VeriSign or its licensors, and you agree to make no claim of interest in or ownership of any such VeriSign Intellectual Property. You acknowledge that no title to the VeriSign Intellectual Property is transferred to you, and that you do not obtain any rights, express or implied, in the VeriSign or its licensors' service, other than the rights expressly granted in this Subscriber Agreement. To the extent that you create any Derivative Work (any work that is based upon one or more preexisting versions of a VeriSign owned or licensed work provided to you, such as an enhancement or modification, revision, translation, abridgement, condensation, expansion, collection, compilation or any other form in which such preexisting works may be recast, transformed or adapted) such Derivative Work shall be owned by VeriSign or its licensors and all right, title and interest in and to each such Derivative Work shall automatically vest in VeriSign or its licensors. VeriSign shall have no obligation to grant you any right in any such Derivative Work. You may not reverse engineer, disassemble or decompile the VeriSign Intellectual Property or make any attempt to obtain source code to the VeriSign Intellectual Property. You have the right to use the Certificate under the terms and conditions of this Subscriber Agreement.

5. Modifications. This Subscriber Agreement may not be modified, and no amendment shall be binding, unless made in writing and signed by you and VeriSign.

6. Warranties.
6.1 VeriSign Warranty.

VeriSign warrants to you that:

(i)There are no misrepresentations of fact in such Certificate known to or originating from VeriSign;

(ii)Any Certificate issued that assert the policy OIDs identified in the VeriSign ECA CPS § 1.2 is issued in accordance with the ECA CP and the Verisign ECA CPS;

(iii)There are no errors in the information in the Certificate that were introduced by VeriSign as a result of its failure to exercise reasonable care in creating the Certificate;

(iv)Such Certificates meet all requirements of the VeriSign ECA CPS;

(v)Revocation services and use of a repository conform to the VeriSign ECA CPS in all respects; and

(vi)Any RA or its Trusted Agent will operate in accordance with the applicable sections of the ECA CP and the VeriSign ECA CPS.

6.2 Your Warranty.

By accepting a ECA Certificate issued by VeriSign, you certify to and agree with VeriSign and to all who rely on the information contained in your Certificate that at the time of acceptance and throughout the operational period of the Certificate, until notified otherwise by you:

(i) each digital signature created using the private key corresponding to the public key listed in the Certificate is your digital signature and the Certificate has been accepted by you and is operational (not expired, suspended or revoked) at the time the digital signature is created;

(ii) you have no knowledge of any unauthorized access to your private key;

(iii) all representations made by you to VeriSign regarding the information contained in the Certificate are correct;

(iv) all information contained in the Certificate is correct to the extent that you had knowledge or notice of such information and you shall promptly notify VeriSign of any material inaccuracies in such information as set forth in the VeriSign ECA CPS § 4.3.1;

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

(vi) you are an end-user and will not use or authorize anyone to use the private key associated with the ECA certificate for signing any Certificate or CRL;

(vii) Generate PINs, passwords, and pass-phrases used to protect the private keys and used in registration and revocation process in accordance with the requirements of the ECA CP and the VeriSign ECA CPS;

(viii) Protect PINs, passwords, and pass-phrases used to protect the private keys and used in registration and revocation process from disclosure to anyone; and

(ix) Install the ECA Root CA trust anchor in accordance with the requirements of the ECA CP and VeriSign ECA CPS.

7. DISCLAIMERS OF WARRANTY AND LIABILITY.

7.1 SPECIFIC DISCLAIMERS

EXCEPT AS OTHERWISE SET FORTH IN THE ECA CP AND THE CPS, VERISIGN:

(I) SHALL NOT INCUR LIABILITY TO ANY PERSON OR ENTITY FOR REPRESENTATIONS CONTAINED IN A CERTIFICATE, PROVIDED THE CERTIFICATE WAS PREPARED 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 OR WILLFUL MISCONDUCT, AND

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

7.2 GENERAL WARRANTY DISCLAIMER

EXCEPT AS SET FORTH IN THE ECA CP AND THE CPS AND THIS SUBSCRIBER AGREEMENT, AND TO THE EXTENT PERMITTED BY APPLICABLE LAW, VERISIGN DISCLAIMS ANY AND ALL OTHER EXPRESS OR IMPLIED WARRANTIES OF ANY TYPE TO ANY PERSON OR ENTITY, 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.

8. LIMITATIONS OF LIABILITY.

8.1 LIMITATIONS ON AMOUNT OF DAMAGES

IN THE EVENT YOU INITIATE ANY CLAIM, ACTION, SUIT, ARBITRATION, OR OTHER PROCEEDING SEPARATE FROM A REQUEST FOR PAYMENT UNDER THE ECA CPS AND TO THE EXTENT PERMITTED BY APPLICABLE LAW, VERISIGN'S LIABILITY SHALL BE LIMITED AS FOLLOWS:

THE TOTAL LIABILITY OF VERISIGN TO ANY PARTY FOR GENERAL CONTRACT, TORT OR ANY OTHER DAMAGES FOR NEGLIGENT, RECKLESS, OR FRAUDULENT CONDUCT BY THE VERISIGN ECA, ITS RAS OR TRUSTED AGENTS IN CONNECTION WITH A SINGLE TRANSACTION INVOLVING THE USE OR RELIANCE ON A CERTIFICATE SHALL BE LIMITED TO ONE THOUSAND DOLLARS ($1,000 USD). FURTHERMORE, VERISIGN'S TOTAL LIABILITY FOR ANY INCIDENT (AGGREGATE OF ALL TRANSACTIONS)

INVOLVING THE USE OR RELIANCE ON A CERTIFICATE SHALL BE LIMITED TO ONE MILLION DOLLARS ($1,000,000 USD). THESE LIABILITY CAPS 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.

8.2 EXCLUSION OF CERTAIN ELEMENTS OF DAMAGES

EXCEPT AS EXPRESSLY PROVIDED IN THE ECA CPS, AND TO THE EXTENT PERMITTED BY APPLICABLE LAW, VERISIGN SHALL NOT BE LIABLE IN CONTRACT TO ANY PERSON OR ENTITY 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 THE ECA 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 OR ENTITY 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 THE ECA CPS.

8.3 U.S. FEDERAL GOVERNMENT LIABILITY

YOU SHALL HAVE NO CLAIM AGAINST THE UNITED STATES FEDERAL GOVERNMENT ARISING FROM USE OF YOUR CERTIFICATE OR A CERTIFICATE MANAGEMENT AUTHORITY'S DETERMINATION TO TERMINATE A CERTIFICATE. IN NO EVENT WILL THE GOVERNMENT BE LIABLE FOR ANY LOSSES, INCLUDING DIRECT OR INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL, OR PUNITIVE DAMAGES, ARISING OUT OF OR RELATING TO ANY CERTIFICATE ISSUED OR REVOKED BY THE VERISIGN ECA.

YOU SHALL HAVE NO CLAIM AGAINST THE U.S. FEDERAL GOVERNMENT ARISING FROM ERRONEOUS CERTIFICATE STATUS INFORMATION PROVIDED BY THE SERVERS AND SERVICES OPERATED BY THE ECA AND BY THE U.S. FEDERAL GOVERNMENT.

9. Force Majeure. Except for payment and indemnity obligations hereunder, neither party shall be deemed in default hereunder, nor shall it hold the other party responsible for, any

delay or failure in the performance of its obligations hereunder from events beyond its control including, but not limited to, acts of God, acts of war, epidemics, power outages, fire, earthquakes, and other disasters, provided that the party relying upon this section (i) shall have given the other party written notice thereof promptly and, in any event, within five (5) business days of discovery thereof; and (ii) shall take all reasonable steps reasonably necessary under the circumstances to mitigate the effects of the force majeure event upon which such notice is based; provided further, that

in the event of a force majeure event described in this section extends for a period in excess of thirty (30) days in the aggregate, the other party may immediately terminate this Subscriber Agreement.

10. Export Control. You agree to conform to applicable export laws and regulations.

11. Severability. You agree that the terms of this Subscriber Agreement are severable. If any term or provision is declared invalid or unenforceable, in whole or in part, that term or provision will not affect the remainder of this Subscriber Agreement; this Subscriber Agreement will be deemed amended to the extent necessary to make this Subscriber Agreement enforceable, valid and, to the maximum extent possible consistent with applicable law, consistent with the original intentions of the parties; and the remaining terms and conditions will remain in full force and effect.

12. 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 Agreement, irrespective of contract or other choice of law provisions and without the requirement to establish a commercial nexus in California. The parties further agree that jurisdiction and venue for any matter arising out or pertaining to this Agreement shall be proper only in the state and federal courts located in Santa Clara County and the Northern District of the State of California, United States of America.

13. Dispute Resolution. To the extent permitted by law, before you invoke any dispute resolution mechanism with respect to a dispute involving any aspect of this Subscriber Agreement, you shall notify VeriSign and any other party to the dispute for the purpose of seeking dispute resolution. If the dispute is not resolved within sixty (60) days after the initial notice, then you may proceed in accordance with the following formal dispute resolution: If you are an individual or entity within the United States Government and have purchased the services associated with this Subscriber Agreement, 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, you may invoke a dispute resolution mechanism as follows.

(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.** All suits to enforce any provision of this Subscriber Agreement or arising in connection with this Subscriber Agreement 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. The parties agree that such courts shall have exclusive in personam jurisdiction and venue and the parties submit to the exclusive in personam jurisdiction and venue of such courts. The parties further waive any right to a jury trial regarding any action brought in connection with this Subscriber Agreement.

(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 this Subscriber Agreement shall be finally settled under the Rules of Conciliation and Arbitration of the International Chamber of Commerce (ICC) as 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. Nothing in this Subscriber Agreement will be deemed as preventing either party from seeking injunctive relief (or any other provisional remedy) from any court having jurisdiction over the parties and the subject matter of this dispute as is necessary to protect either party's name, proprietary information, trade secret, know-how, or, or any other intellectual property rights.

14. Non-Assignment. Except as otherwise set forth herein, your rights under this Subscriber Agreement are not assignable or transferable. Any attempt by your creditors to obtain an interest in your rights under this Subscriber Agreement, whether by attachment, levy, garnishment or otherwise, renders this Subscriber Agreement voidable at VeriSign's option.

15. Notices. You shall make all notices, demands, or requests to VeriSign with respect to this Subscriber Agreement in writing to: VeriSign, Inc., 487 East Middlefield Road, Mountain View, CA 94043, USA, Attention: Practices, with a copy to the General Counsel at the same address.

16. Survival. This Subscriber Agreement shall be applicable for as long as the Certificate remains valid.

17. Privacy. You agree that VeriSign may place in your Certificate certain information that you provide for inclusion in your Certificate. You also agree that VeriSign may publish your Certificate and information about its status in the VeriSign ECA repository and make this information available to relying parties.

18. Conflict of Provisions. In the event of a conflict between this Subscriber Agreement, the VeriSign ECA CPS and other rules, guidelines, or contracts, the Subscriber shall be bound by the provisions of the ECA CP and the VeriSign ECA CPS except to the extent that the provisions of the ECA CP and the VeriSign CPS are prohibited by law. In the event of a conflict between the ECA CP and the VeriSign CPS, the ECA CP shall take precedence over the VeriSign ECA CPS.

19. Entire Agreement. This Subscriber Agreement, together with the ECA CP and KRP, and the VeriSign ECA CPS and KRPS, constitutes the entire understanding and agreement between VeriSign and you with respect to the transactions contemplated, and supersedes any and all prior or contemporaneous oral or written representation, understanding, agreement or communication between VeriSign and you concerning the subject matter hereof. Neither party is relying upon any warranties, representations, assurances or inducements not expressly set forth herein.

20. **Effect of a Certificate.** You acknowledge and understand that your ECA Identity Certificate may be used to digitally sign certain instruments that can be signed using a handwritten signature and doing so may lead to enforceable obligations.

ECA Subscriber Agreement v1.0 (January 2005)