

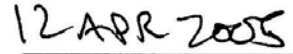


**X.509 CERTIFICATE POLICY FOR THE
U.S. DEPARTMENT OF HOMELAND SECURITY
PUBLIC KEY INFRASTRUCTURE (PKI)**

April 6, 2005
Version 2.3

SIGNATURE PAGE





*Department of Homeland Security Public Key Infrastructure
Policy Authority*

Date

CONTENTS

1.0	INTRODUCTION.....	1
1.1	Purpose.....	1
1.2	Overview.....	1
1.2.1	Certificate Policy	1
1.2.2	Relationship Between the DHS CP and the DHS CP Statement	2
1.2.3	Relationship Between the FBCA CP and the DHS CP.....	2
1.3	Identification.....	2
1.4	Community and Applicability.....	2
1.4.1	PKI Authorities	2
1.4.2	Related Authorities	5
1.4.3	End Entities.....	6
1.4.4	Applicability	6
1.5	Contact Details.....	10
1.5.1	Specification Administration Organization	10
1.5.2	Contact Person	10
1.5.3	Person Determining Certification Practice Statement Suitability for the Policy	10
2.0	GENERAL PROVISIONS.....	10
2.1	Obligations.....	10
2.1.1	CA Obligations	10
2.1.2	RA/LRA Obligations	11
2.1.3	Subscriber Obligations.....	12
2.1.4	Relying Party Obligations.....	12
2.1.5	Repository Obligations	12
2.1.6	Certificate Status Authority Obligations.....	13
2.2	Liability.....	13
2.3	Financial Responsibility.....	13
2.3.1	Indemnification by Relying Parties and Subscribers	13
2.3.2	Fiduciary Relationships	13
2.3.3	Governing Law	13
2.3.4	Administrative Processes	13
2.4	Interpretation and Enforcement	14
2.4.1	Severability of Provisions, Survival, Merger, and Notice	14
2.4.2	Dispute Resolution Procedures	14
2.5	Fees	14
2.6	Publication and Repository.....	14
2.6.1	Publication of CA Information	14
2.6.2	Frequency of Publication	14
2.6.3	Access Controls	14
2.6.4	Repositories.....	14
2.7	Compliance Audit	15
2.7.1	Frequency of Entity Compliance Audit	15
2.7.2	Identity/Qualifications of Compliance Auditor	15

2.7.3	Compliance Auditor’s Relationship to Audited Party	15
2.7.4	Topics Covered by Compliance Audit.....	15
2.7.5	Actions Taken as a Result of Deficiency	16
2.7.6	Communication of Result	16
2.8	Confidentiality	16
2.8.1	Types of Information to be Kept Confidential.....	16
2.8.2	Types of Information Not Considered Confidential	16
2.8.3	Disclosure of Certificate Revocation/Suspension Information.....	17
2.8.4	Release to Law Enforcement Officials	17
2.8.5	Release as Part of Civil Discovery.....	17
2.8.6	Disclosure Upon Owner’s Request.....	17
2.8.7	Other Information Release Circumstances	17
2.9	Intellectual Property Rights	17
3.0	IDENTIFICATION AND AUTHENTICATION	17
3.1	Initial Registration	17
3.1.1	Types of Names	17
3.1.2	Need for Names to be Meaningful.....	18
3.1.3	Rules for Interpreting Various Name Forms	18
3.1.4	Uniqueness of Names	18
3.1.5	Name Claim Dispute Resolution Procedure	18
3.1.6	Recognition, Authentication and Role of Trademarks	18
3.1.7	Method to Prove Possession of Private Key	18
3.1.8	Authentication of Organization Identity	19
3.1.9	Authentication of Individual Identity.....	19
3.1.10	Authentication of Component Identities.....	21
3.2	Routine Re-key, Certificate Renewal, and Update	22
3.3	Obtaining a New Certificate After Revocation.....	23
3.4	Revocation Request	23
4.0	OPERATIONAL REQUIREMENTS.....	23
4.1	Application for a Certificate	23
4.1.1	Cross-Certification Certificate Application	23
4.1.2	Subordinate CA Certificate Application.....	24
4.1.3	Subscriber Certificate Application.....	25
4.1.4	Delivery of Public Key for Certificate Issuance	26
4.2	Certificate Issuance.....	26
4.2.1	Delivery of Subscriber’s Private Key to Subscriber	27
4.2.2	CA Public Key Delivery	27
4.3	Certificate Acceptance	27
4.4	Certificate Revocation and Suspension	28
4.4.1	Circumstances for Revocation or Suspension.....	28
4.4.2	Who Can Request Revocation or Suspension.....	29
4.4.3	Procedure for Revocation or Suspension Request	29
4.4.4	Revocation Request Grace Period	30
4.4.5	Certificate Revocation Lists.....	30
4.4.6	CRL Checking Requirements	30
4.4.7	Online Revocation Status Checking	31

4.4.8	Other Forms of Revocation Checking	31
4.5	Security Audit Procedure.....	31
4.5.1	Types of Events Recorded	31
4.5.2	Frequency of Processing Data	34
4.5.3	Retention Period for Audit Log	35
4.5.4	Protection of Audit Log	35
4.5.5	Audit Log Backup Procedures	35
4.5.6	Audit Collection System (Internal vs. External).....	35
4.5.7	Notification to Event-Causing Subject	35
4.5.8	Vulnerability Assessments.....	35
4.6	Records Archival	36
4.6.1	Types of Events Archived.....	36
4.6.2	Retention Period for Archive	37
4.6.3	Protection of Archive.....	37
4.6.4	Archive Backup Procedures.....	37
4.6.5	Requirements for Time Stamping of Records	37
4.6.6	Archive Collection System (Internal and External).....	37
4.6.7	Procedures to Obtain and Verify Archive Information.....	38
4.7	Key Changeover.....	38
4.7.1	Certificate Re-key	38
4.7.2	Certificate Recovery	38
4.7.3	Certificate Update	38
4.8	Compromise and Disaster Recovery.....	39
4.9	CA Termination	39
5.0	PHYSICAL, PROCEDURAL AND PERSONNEL SECURITY CONTROLS	40
5.1	Physical Controls for a DHS CA	40
5.1.1	Site Location and Construction.....	40
5.1.2	Physical Access.....	40
5.1.3	Electrical Power	41
5.1.4	Water Exposures	41
5.1.5	Fire Prevention and Protection.....	41
5.1.6	Media Storage	41
5.1.7	Waste Disposal.....	41
5.1.8	Off-Site Backup	42
5.2	Procedural Controls	42
5.2.1	Trusted Roles	42
5.2.2	Separation of Roles	43
5.2.3	Number of Persons Required per Task	44
5.2.4	Identification and Authentication for Each Role	44
5.3	Personnel Controls	44
5.3.1	Background, Qualifications, Experience, and Security Clearance Requirements	44
5.3.2	Background Check Procedures	45
5.3.3	Training Requirements.....	45
5.3.4	Retraining Frequency and Requirements.....	45
5.3.5	Job Rotation Frequency and Sequence	45

- 5.3.6 Sanctions for Unauthorized Actions45
- 5.3.7 Contracting Personnel Requirements.....45
- 5.3.8 Documentation Supplied to Personnel.....45
- 6.0 TECHNICAL SECURITY CONTROLS46**
 - 6.1 Key Pair Generation and Installation46
 - 6.1.1 Key Pair Generation.....46
 - 6.1.2 Private Key Delivery to Subscriber46
 - 6.1.3 Public Key Delivery to Certificate Issuer47
 - 6.1.4 CA Public Key Delivery to Users.....47
 - 6.1.5 Key Sizes47
 - 6.1.6 Public Key Parameters Generation48
 - 6.1.7 Parameter Quality Checking48
 - 6.1.8 Hardware/Software Key Generation.....48
 - 6.1.9 Key Usage.....48
 - 6.2 Private Key Protection48
 - 6.2.1 Standards for Cryptographic Module.....48
 - 6.2.2 Private Key Multi-Person Control49
 - 6.2.3 Private Key Escrow.....49
 - 6.2.4 Private Key Backup49
 - 6.2.5 Private Key Archival.....50
 - 6.2.6 Private Key Entry into Cryptographic Module.....50
 - 6.2.7 Method of Activating Private Keys50
 - 6.2.8 Methods of Deactivating Private Keys51
 - 6.2.9 Method of Destroying Subscriber Private Signature Keys.....51
 - 6.3 Other Aspects of Key-Pair Management51
 - 6.3.1 Public Key Archival.....51
 - 6.3.2 Usage Periods for the Public and Private Keys51
 - 6.4 Activation Data52
 - 6.4.1 Activation Data Generation and Installation.....52
 - 6.4.2 Activation Data Protection.....52
 - 6.4.3 Other Aspects of Activation Data.....52
 - 6.5 Computer Security Controls53
 - 6.5.1 Specific Computer Security Technical Requirements53
 - 6.5.2 Computer Security Rating.....53
 - 6.6 Lifecycle Technical Controls.....53
 - 6.6.1 System Development Controls54
 - 6.6.2 Security Management Controls.....54
 - 6.7 Network Security Controls54
 - 6.8 Cryptographic Module Engineering Controls.....54
- 7.0 CERTIFICATE AND CRL PROFILES.....55**
 - 7.1 Certificate Profile.....55
 - 7.1.1 Version Numbers55
 - 7.1.2 Certificate Extensions55
 - 7.1.3 Algorithm Object Identifiers.....55
 - 7.1.4 Name Forms.....55
 - 7.1.5 Name Constraints.....56

7.1.6	Certificate Policy Object Identifier	56
7.1.7	Usage of Policy Constraints Extension	56
7.1.8	Policy Qualifiers Syntax and Semantics	56
7.1.9	Processing Semantics for the Critical Certificate Policy Extension	56
7.2	CRL Profile	56
7.2.1	Version Numbers	56
7.2.2	CRL Entry Extensions	56
8.0	SPECIFICATION ADMINISTRATION	56
8.1	Specification Change Procedures	56
8.2	Publication and Notification Policies.....	57
8.3	CPS Approval Procedures.....	57
8.4	Waivers	57

ATTACHMENT A—ACRONYMS AND ABBREVIATIONS

ATTACHMENT B—GLOSSARY

ATTACHMENT C—REFERENCES

EXHIBITS

Exhibit 1:	Registered Certificate Policy Object Identifiers	2
Exhibit 2:	Levels of Assurance	7
Exhibit 3:	Identification Requirements	21
Exhibit 4:	Routine Re-key and Certificate Renewal Identity Requirements for Subscriber Signature and Encryption Certificates	22
Exhibit 5:	Auditable Events	32
Exhibit 6:	Audit Log Review Schedule	34
Exhibit 7:	Archive Requirements.....	36
Exhibit 8:	Archive Retention Schedule.....	37
Exhibit 9:	Role Separation Requirements.....	43
Exhibit 10:	Minimum Acceptable Key Lengths	47
Exhibit 11:	Minimum Requirements for Cryptographic Modules.....	49
Exhibit 12:	Maximum Permissible Private Key and Certificate Lifetimes	52
Exhibit 13:	Signature Object Identifiers	55
Exhibit 14:	Algorithm Object Identifiers	55

1.0 INTRODUCTION

1.1 Purpose

The Department of Homeland Security (DHS) will implement a Public Key Infrastructure (PKI) to increase the security posture of the organization. The PKI consists of products and services that provide and manage X.509 public key certificates. The PKI will bind its Subscribers (as defined in Section 1.3.3.1) to public/private key pairs, through the use of these X.509 certificates. Public key certificates identify the Subscriber named in the certificate and bind that identity to a public key embedded in the certificate. Every public key certificate issued by the DHS PKI and asserting one of the policies listed in Section 1.3 shall be issued under the applicable requirements of this Certificate Policy (CP).

This CP addresses five different assurance levels (Test, Rudimentary, Basic, Medium, and High) for public key certificates. The word “assurance” used in this CP means how well a Relying Party can be certain of the identity binding between the public key and the individual whose subject name is cited in the certificate. In addition, it also reflects how well the Relying Party can be certain that the individual whose subject name is cited in the certificate is controlling the use of the private key that corresponds to the public key in the certificate, and how securely the system that was used to produce the certificate and (if appropriate) deliver the private key to the Subscriber performs its task.

The DHS PKI consists of an off-line DHS Root Certification Authority (CA), one or more subordinate DHS CAs at one or more of the five different assurance levels (Test, Rudimentary, Basic, Medium, and High), and the Registration Authorities (RA), Local Registration Authorities (LRA) and Subscribers associated with these CAs. The DHS Root CA shall act the Principal CA (PCA) for cross certification with the Federal Bridge CA (FBCA) to achieve interoperability with other entity PKIs that have also cross certified with the FBCA.

This CP is compliant with the FBCA Policy, and the FBCA High, Medium, Basic, Rudimentary and Test assurance-level definitions.

This DHS CP is consistent with the Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (IETF PKIX) Request for Comment (RFC) 2527, Certificate Policy and Certification Practice Statement Framework.

The terms and provisions of this DHS CP shall be interpreted under and governed by applicable Federal law.

1.2 Overview

This document defines the policy under which the DHS PKI will be established and operate.

1.2.1 Certificate Policy

This document contains CPs for five assurance levels. DHS PKI issued public key certificates shall contain a certificate policy Object Identifier (OID), registered with the Computer Security Objects Registry (CSOR) that shall identify the CP (assurance level) under which the public key certificates were issued. The party that registers the OID (in this case, the DHS) also publishes the CP, for examination by relying parties. Public key certificates issued by the DHS Root CA

to CAs outside the DHS PKI shall, in the *policyMappings* extension, identify the equivalent policies of certified CAs.

1.2.2 Relationship Between the DHS CP and the DHS CP Statement

The DHS CP states what assurance can be placed in a certificate issued by the DHS. The DHS CP Statement (CPS) states how the DHS establishes that assurance.

1.2.3 Relationship Between the FBCA CP and the DHS CP

The levels of assurance of the certificates issued under the FBCA CP are mapped by the Federal PKI Policy Authority to the levels of assurance of the certificates issued by the DHS CAs. The policy mappings information is placed into the certificates issued by the FBCA, in order to facilitate interoperability. As stated in Section 1.2.1, the DHS Root CA places the policy mapping information in the certificates it issues to the CAs outside the DHS PKI domain.

1.3 Identification

There are five levels of assurance in this Certificate Policy that are defined in subsequent sections. Each level of assurance has an OID, to be asserted in certificates issued by the DHS PKI. The OIDs are registered under the id-infosec arc as listed in Exhibit 1.

Exhibit 1: Registered Certificate Policy Object Identifiers

Level of Assurance Identifier	OID
csor-certpolicy OBJECT IDENTIFIER	::= {2 16 840 1 101 3 2 1 }
dhs-policies OBJECT IDENTIFIER	::= {csor-certpolicy 15}
id-dhs-certpcy-rudimentaryAssurance	::= dhs-policies 1
id-dhs-certpcy-basicAssurance	::= dhs-policies 2
id-dhs-certpcy-mediumAssurance	::= dhs-policies 3
id-dhs-certpcy-highAssurance	::= dhs-policies 4
id-dhs-certpcy-testRudimentaryAssurance	::= dhs-policies 31
id-dhs-certpcy-testBasicAssurance	::= dhs-policies 32
id-dhs-certpcy-testMediumAssurance	::= dhs-policies 33
id-dhs-certpcy-testHighAssurance	::= dhs-policies 34

1.4 Community and Applicability

This section describes roles relevant to the administration and operation of the DHS PKI.

1.4.1 PKI Authorities

1.4.1.1 DHS PKI Policy Authority

The DHS Chief Information Security Officer is the DHS PKI Policy Authority (PA), i.e.,

Robert Charles West
DHS PKI Policy Authority

Department of Homeland Security
7th and D Street SW
Washington, DC 20528

The DHS PKI Policy Authority is responsible for the following:

- Creation, maintenance and publication of all CPs pertaining to the DHS PKI
- Approving all cross certifications by DHS Root or Subordinate CAs
- Executing a Memorandum of Agreement (MOA) between the DHS and any Entity wishing to cross certify with a DHS CA. The MOA shall set forth the respective responsibilities and obligations of both parties, and the mappings between the certificate levels of assurance contained in this CP and those in the Entity CP. Thus, the term “MOA,” as used in this CP, shall always refer to the Memorandum of Agreement cited in this paragraph. When the entity belongs to a sovereign nation, the United States Department of State may execute the MOA or delegate the authority to execute the MOA on its behalf
- Ensuring continued conformance of all cross-certified Entities with applicable requirements as set forth in the MOA as a condition for allowing continued cross certification with a DHS Certification Authority
- Appointing a DHS Operational Authority (OA)
- Appointing an Alternate DHS PKI Policy Authority to fill the DHS PKI Policy Authority role, in the event that the DHS PKI Policy Authority is not available, or unable to perform the duties assigned by this CP
- Appointing an Alternate DHS PKI Operational Authority to fill the DHS PKI Operational Authority role, in the event that the DHS PKI Operational Authority is not available, or unable to perform the duties assigned by this CP

The DHS PKI Policy Authority hereby appoints the following:

- The DHS PKI Operational Authority is:
William Morgan, Jr.
Department of Homeland Security
1616 North Fort Meyer Drive
Arlington, VA 22209
- The Alternate DHS PKI Policy Authority is:
Don Hagerling
Department of Homeland Security
7th and D Street SW
Washington, DC 20528
- The Alternate DHS PKI Operational Authority is:
G. E. Woodford
Department of Homeland Security
801 I Street NW
Washington, DC 20536

1.4.1.2 Certification Authority

A Certification Authority is an entity that includes personnel (Operational Authority [OA]), hardware, and software that will create, sign, issue, manage, and store public key certificates and Certificate Revocation Lists (CRL).

CAs are ultimately responsible for ensuring that the certificates they sign are generated and managed in accordance with this policy.

As “CA” is used throughout this CP, it may refer to the CA hardware, CA software, the personnel who operate the CA, or any combination of these three elements.

1.4.1.2.1 Principal CA

The Principal CA is a CA within the DHS PKI that has been designated to cross-certify directly with the FBCA, and which issues either end-entity certificates, CA certificates, or cross-certificates to other CAs. The DHS PKI shall have one Principal CA, referred to as the “Root CA.” Additionally, this CP refers to CAs that are “subordinate” to the Principal CA.

1.4.1.3 DHS PKI Operational Authority

The DHS Operational Authority is a DHS official, appointed by the DHS PKI PA, who oversees the proper operation of the DHS PKI, and reports to the DHS PKI PA on PKI-related matters.

The DHS PKI Operational Authority is as follows:

William Morgan, Jr.
DHS PKI Operational Authority
Department of Homeland Security
1616 North Fort Meyer Drive
Arlington, VA 22209

The DHS PKI Operational Authority is responsible for the following:

- Creation and maintenance of all PKI CPSs pertaining to the DHS PKI
- Creation and management of DHS PKI Operating Procedures
- Management of DHS PKI Operations, including all aspects of the issuance and management of a certificate; e.g.,:
 - Control over the registration process
 - The certificate manufacturing process
 - Publication of certificates
 - Revocation of certificates
 - Generation and destruction of CA signing keys
 - Re-key of CA
 - Ensuring that all aspects of DHS PKI services, operations and infrastructure related to certificates issued under this CP are in accordance with the requirements, representations, and warranties of this CP

1.4.1.4 Registration Authority/Local Registration Authority

The Registration Authority (RA) is the entity that collects and verifies each Subscriber's identity and information that are to be entered into the Subscriber's public key certificate. The RA performs its function in accordance with a CPS approved by the DHS PKI Policy Authority. The RA may delegate this responsibility to an Local Registration Authority (LRA). The RA is responsible for:

- Control over the registration process
- The identification and authentication process

1.4.1.5 Trusted Agents

Trusted Agents (TA) perform the face-to-face Subscriber authentication. Use of a TA is optional. They can be used where convenient to reduce the demands on an RA or an LRA. The trusted agent concept allows easier registration of Subscribers at remote locations, where it may be impractical for the Subscriber to visit an LRA in-person or vice versa. TAs may provide certificate registration instructions to Subscribers, check the Subscriber applicant's IDs (e.g., government-issued photo ID) before the registration instructions are provided and ensure that the Subscriber signs the Subscriber Agreement.

1.4.1.6 Certificate Status Authority

A Certificate Status Authority (CSA) is the collection of hardware, software and operation personnel that run a DHS service to provide the status of a DHS issued certificate. Examples of CSA are as follows:

- Online Certificate Status Protocol (OCSP) Responder used to obtain the revocation status of a DHS issued certificate
- Simple Certificate Validation Protocol (SCVP) Server used to develop and validate a certificate path on behalf of a DHS relying party

1.4.1.7 Security Compliance Officer

The Security Compliance Officer (SCO) is responsible for performing ongoing audit oversight of CA operations on behalf of the DHS PKI Policy Authority and DHS PKI Operational Authority, to ensure compliance with this CP, the CA's CPS and the CA's operating procedures.

1.4.2 Related Authorities

1.4.2.1 Federal Bridge Certification Authority

The FBCA is the CA operated by the FBCA OA and issues certificates to the various U.S. Federal department and agency PCAs. The FBCA was established to provide an infrastructure capability to facilitate trust between commercial and Government agencies wishing to exchange information securely. The DHS Root CA shall cross-certify with the FBCA to enable secure communications with external communities of interest.

1.4.3 End Entities

1.4.3.1 Subscribers

A Subscriber is the entity (human, device, application, organization, etc.) whose name appears as the subject in a certificate, who asserts that it uses its key and certificate in accordance with the certificate policy asserted in the certificate, and who does not itself issue certificates.

Subscribers include both human users and non-human system components, such as servers, network appliances, and application processes.

DHS human Subscribers may include the following:

- DHS employees
- DHS contractors
- Authorized personnel from other government, business, academic organizations
- Authorized U.S. citizens
- Authorized non U.S. citizens

1.4.3.2 Relying Parties

A Relying Party is the entity that relies on the validity of the binding of the Subscriber's name to a public key. The Relying Party is responsible for deciding whether or how to check the validity of the certificate by checking the appropriate certificate status information. The Relying Party can use the certificate to verify the integrity of a digitally signed message, to identify the creator of a message, or to establish confidential communications with the subject of the certificate. 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.

1.4.3.3 PKI Sponsor

A PKI Sponsor fills the role of a Subscriber for non-human system components that are named as public key certificate subjects. The PKI Sponsor works with the RAs to register components (routers, firewalls, etc.) in accordance with Section 3.1.10, and shall be responsible for meeting the obligations of Subscribers as defined throughout this document.

1.4.4 Applicability

The sensitivity of the information protected using certificates issued by the DHS PKI will vary significantly. Entities must evaluate their environment and the associated threats and vulnerabilities and determine the level of risk they are willing to accept based on the sensitivity or significance of the information involved. This evaluation is done by each Entity for each application and is not controlled by this CP.

To provide sufficient granularity, this CP specifies security requirements at four increasing, qualitative levels of assurance: Rudimentary, Basic, Medium and High. The DHS PKI is intended to support applications involving unclassified information, which can include sensitive unclassified data protected pursuant to Federal statutes and regulations.

The certificate levels of assurance contained in this CP are set forth in Exhibit 2, as well as a brief and non-binding description of the applicability for applications suited to each level.

Exhibit 2: Levels of Assurance

Assurance Level	Applicability
Test	This level is to be used for testing purposes only. There is no assurance associated with this level. This level includes the following Policy OIDs: <ul style="list-style-type: none"> • 2 16 840 1 101 3 2 1 15 31 • 2 16 840 1 101 3 2 1 15 32 • 2 16 840 1 101 3 2 1 15 33 • 2 16 840 1 101 3 2 1 15 34
Rudimentary	This level provides the lowest degree of assurance concerning identity of the individual. One of the primary functions of this level is to provide data integrity to the information being signed. This level is relevant to environments in which the risk of malicious activity is considered to be low. It is not suitable for transactions requiring authentication, and is generally insufficient for transactions requiring confidentiality, but may be used for the latter where certificates having higher levels of assurance are unavailable.
Basic	This level provides a basic level of assurance relevant to environments where there are risks and consequences of data compromise, but they are not considered to be of major significance. This may include access to private information where the likelihood of malicious access is not high. It is assumed at this security level that users are not likely to be malicious.
Medium	This level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial.
High	This level is appropriate for use where the threats to data are high, or the consequences of the failure of security services are high. This may include very high value transactions or high levels of fraud risk.

1.4.4.1 DHS Test Assurance

The DHS Test assurance and the FBCA Test assurance levels map directly. This level is suitable for testing and evaluation purposes only. This level is not suitable for any transactions that require authentication or confidentiality. The remainder of this Policy does not apply to certificates expressing the Test assurance level.

1.4.4.2 DHS Rudimentary Assurance

The DHS Rudimentary assurance and FBCA Rudimentary assurance levels map directly. This level is relevant to environments in which the risk of malicious activity is considered to be low. It is not suitable for transactions requiring authentication, and is generally insufficient for transactions requiring confidentiality, but may be used for the latter where certificates having

higher levels of assurance are unavailable. In particular, an authentication error of a user's identity at Rudimentary assurance should result in at most:

- Minimal inconvenience to any party
- Minimal financial loss to any party
- Minimal distress being caused to any party
- Minimal damage to any party's standing or reputation
- No release of personal, U.S. government sensitive, or commercially sensitive data to third parties
- No risk that an egregious criminal act will occur in the transaction, or that the transaction will assist materially in the commission or concealment of a egregious criminal act
- No risk to any party's personal safety

1.4.4.3 DHS Basic Assurance

The DHS Basic assurance and FBCA Basic assurance level map directly. This policy assurance level is intended to support low value unclassified data of no significant financial value. This level is established to support interaction with Industry and Business Partners over public networks such as the Internet. This level is required when a relationship with an entity or a party must be ascertained for low value and non-sensitive transactions such as for bi-directional SSL authentication.

Basic assurance is appropriate for transactions where it is sufficient that there exists reasonable confidence in the asserted electronic identity of the transacting party. In particular, an authentication error of a user's identity at Basic assurance might result in:

- Minor inconvenience to any party
- Minor financial loss to any party
- Minor damage to any party's standing or reputation
- Minor distress being caused to any party
- No release of personal, U.S. government sensitive, or commercially sensitive data to third parties
- No risk that an egregious criminal act will occur in the transaction, or that the transaction will assist materially in commission or concealment of an egregious criminal act
- No risk to any party's personal safety

1.4.4.4 DHS Medium Assurance

The DHS Medium assurance and the FBCA Medium assurance level map directly. This policy assurance level is intended to support low to medium value sensitive-but-unclassified (SBU) data in high-risk network environments or unclassified (SBU) data of moderate to high organizational or financial value in secure low risk network environments (requires hardware tokens). This level is the lowest level of assurance that may be supported by the DHS Medium assurance for

receipt of electronic data submissions from Industry, Business Partners, and other Federal government agencies that require the evidence of non-repudiation from legally binding digital signatures.

Medium assurance is appropriate for transactions that are official in nature, and for which there is a need for high confidence in the asserted electronic identity of the transacting party. In particular, an authentication error of a user's identity at Medium assurance might result in the following:

- Significant inconvenience to any party
- Significant financial loss to any party
- Significant damage to any party's standing or reputation
- Significant distress being caused to any party
- Release of some personal, U.S. government sensitive data or commercially sensitive to third parties
- Significant risk that an egregious criminal act will occur in the transaction, or that the transaction will assist materially in the commission or concealment of an egregious criminal act

1.4.4.5 DHS High Assurance

The DHS High assurance and the FBCA High assurance level map directly. This policy assurance level is intended to support medium to high value SBU data in high-risk external environments. This level is required for any instances where the identity of an individual is required for authorization or acknowledgement of high value sensitive electronic transactions.

High assurance is appropriate for transactions that are official in nature for which there is a need for very high confidence in the asserted electronic identity of the transacting party. In particular, an authentication error of a user's identity at High assurance might result in:

- Considerable inconvenience to any party
- Considerable financial loss to any party
- Considerable damage to any party's standing or reputation
- Considerable distress being caused to any party
- Release of extensive personal, U.S. government-sensitive, commercially-sensitive data, or classified data to third parties
- Considerable risk that an egregious criminal act will occur in the transaction, or that the transaction will assist materially in the commission or concealment of an egregious criminal act
- Risk to any party's personal safety

1.4.4.6 Factors in Determining Usage

The Relying Party must determine the level of assurance required for an application, i.e., select the certificate appropriate for meeting the needs of that application. This shall be determined by

evaluating various risk factors including the value of the information, the threat environment, and the existing protection of the information environment. These determinations are made by the Relying Party and are not controlled by the DHS PKI Policy Authority or the DHS PKI Operational Authority.

1.5 Contact Details

1.5.1 Specification Administration Organization

The DHS PKI Policy Authority is responsible for all aspects of this CP.

1.5.2 Contact Person

Questions, comments and suggestions regarding this CP shall be directed to the DHS PKI Policy Authority, whose address is as follows:

Robert Charles West
DHS PKI Policy Authority
Department of Homeland Security
7th and D Street SW
Washington, DC 20528

1.5.3 Person Determining Certification Practice Statement Suitability for the Policy

CPS approval is the responsibility of the DHS PKI Policy Authority. The DHS PKI PA shall determine the suitability and compliance of any CPS to this policy. Additionally, the DHS PKI PA shall determine if the CPS properly adheres to the policy mappings approved by the Federal PKI Policy Authority between the FBCA CP and this CP.

2.0 GENERAL PROVISIONS

2.1 Obligations

2.1.1 CA Obligations

A DHS CA who issues certificates that assert a policy defined in this document shall conform to the stipulations of this document, including:

- Providing to the DHS PKI PA a CPS, as well as any subsequent changes, for conformance assessment
- Conforming to the stipulations of the approved CPS
- Ensuring that registration information is accepted only from properly authenticated RAs, LRAs, and/or TAs who understand and are obligated to comply with this policy
- Posting newly issued certificates:
 - Including only valid and appropriate information in certificates, and maintaining evidence that due diligence was exercised in validating the information contained in the certificates

- Revoking the certificates of Subscribers found to have acted in a manner counter to those obligations
 - Ensuring that obligations are imposed on non-U.S. Government Subscribers in accordance with the provisions of Section 2.1.3
 - Operating or providing for the services of an online repository that satisfies the obligations under Section 2.1.5, and informing the repository service provider of those obligations if applicable
- Notifying the Subscribers of the issuance of their certificates
 - Notifying the Subscribers of the revocation or suspension of their certificates
 - Processing revocation and suspension requests in a timely manner
 - Posting a listing of revoked and suspended certificates in a timely manner
 - Maintaining certificates and certificate request information
 - Operating or providing for the services of an on-line repository

Some obligations that are defined as CA's may actually be carried out by an RA, on behalf of the CA, but the CA remains ultimately responsible for such obligations.

2.1.2 RA/LRA Obligations

An RA who performs registration functions as described in this document shall comply with the stipulations of this document, and comply with the pertinent CPS approved by the DHS PKI PA for use with this policy. An RA who is found to have acted in a manner inconsistent with these obligations is subject to revocation of RA responsibilities and possible disciplinary action.

An RA shall conform to the stipulations of this document, including:

- Obtaining registration or revocation information from users
- Authenticating users
- Forwarding the results to the CA
- Including only valid and appropriate information in certificate requests, and maintaining evidence that due diligence was exercised in validating the information contained in the certificate
- Ensuring that obligations are imposed on Subscribers in accordance with the Subscriber Obligations (Section 2.1.3), and that Subscribers are informed of the consequences of not complying with those obligations

RAs may delegate user registration and authentication to LRAs. An LRA who performs registration functions as described in this document shall comply with the stipulations of this document, and comply with the pertinent CPS approved by the DHS PKI PA for use with this policy. An LRA who is found to have acted in a manner inconsistent with these obligations is subject to revocation of LRA responsibilities and possible disciplinary action.

2.1.3 Subscriber Obligations

At a minimum, a Subscriber represents and warrants to the CA that it shall:

- Provide correct information to the Registrar without errors, omissions, or misrepresentations
- Exercise diligence in protecting their private keys and cryptographic tokens at all times against loss, theft or tampering
- Use certificates exclusively for legal and authorized purposes in accordance with the terms and conditions of this CP and applicable laws
- Read, understand and abide by all the terms, conditions, and restrictions in the appropriate Subscriber Agreement

Additional Subscriber obligations may be documented in the appropriate Subscriber Agreement, which each Subscriber is required to indicate acceptance of, prior to certificate issuance.

PKI Sponsors assume the obligations of Subscribers for the certificates associated with their components.

2.1.4 Relying Party Obligations

Parties who rely upon the certificates issued under this policy are obligated to perform the following:

- Use the certificate exclusively for authorized purposes for which it was issued, consistent with this policy
- Check each certificate for validity, prior to reliance
- Perform cryptographic operations properly
- Verify the certification path in accordance with the requirements of the X.509 standard
- Preserve the original signed data, the applications necessary to read and process the data, and the cryptographic applications needed to verify the digital signatures on that data as long as it may be necessary to verify the signature on the data

2.1.5 Repository Obligations

The Repository is obligated to perform the following:

- Post to an X.500 Directory Server System that is also accessible through the Lightweight Directory Access Protocol (LDAP)
- Publish and archive certificates
- Publish and archive CRLs/Authority Revocation Lists (ARL)
- Publish and archive the DHS PKI CP
- Post all PKI provided information in a timely manner
- Maintain security to prevent unauthorized access and tampering
- Maintain the availability of the information as required by the certificate information posting and retrieval stipulations of this CP

- Provide access control mechanisms when needed to protect repository information as described in later sections

2.1.6 Certificate Status Authority Obligations

A CSA who provides revocation status and/or complete validation of certificates that assert a policy defined in this document shall conform to the stipulations of this document, including:

- Providing to the DHS PKI PA a CPS, as well as any subsequent changes, for conformance assessment
- Conforming to the stipulations of the approved CPS
- Ensuring that certificate and revocation information is accepted only from CAs trusted by DHS
- Maintaining evidence that due diligence was exercised in validating the 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

The U.S. Government shall not be liable to any party, except as determined pursuant to the Federal Tort Claims Act (FTCA), 28 U.S.C. 2671-2680, or as determined through a valid express written contract between the Government and another party.

2.3 Financial Responsibility

This CP contains no limits on the use of certificates issued by CAs under this policy. Rather, entities, acting as Relying Parties, shall determine what financial limits, if any, they wish to impose for certificates used to consummate a transaction.

2.3.1 Indemnification by Relying Parties and Subscribers

No stipulation.

2.3.2 Fiduciary Relationships

No stipulation.

2.3.3 Governing Law

The terms and provisions of this CP shall be interpreted under and governed by the laws of the United States of America.

2.3.4 Administrative Processes

Administrative processes pertaining to this CP shall be determined by the DHS PKI OA pursuant to the agreement between it and the DHS PKI PA for the operation of the DHS PKI.

2.4 Interpretation and Enforcement

2.4.1 Severability of Provisions, Survival, Merger, and Notice

Should it be determined that one section of this CP is incorrect or invalid, the other sections of this CP shall remain in effect until the CP is updated. The process for updating this CP is described in Section 8.1.

2.4.2 Dispute Resolution Procedures

Procedures to resolve disputes with a CA's operations shall be documented in the CA's CPS. The DHS PKI PA is the final authority to resolve disputes when the CPS procedures do not provide a resolution.

2.5 Fees

The DHS PKI PA reserves the right to impose fees for any or all services provided.

2.6 Publication and Repository

2.6.1 Publication of CA Information

For the use of its Subscribers and Relying Parties, DHS CA(s) shall publish the following information to the repository:

- Issued certificates
- CRLs/ARLs
- The CA's certificate associated with its signing key
- This Certificate Policy
- Any relevant information that is necessary for reliance on certificates issued under this policy

DHS CAs shall not publish their CPS to the repository.

2.6.2 Frequency of Publication

All information to be published in the repository shall be published as soon as such information is available to the CA. Certificates are published immediately following user acceptance as specified in Section 4.2 and proof of possession of private key as specified in Section 3.1.7. Information regarding frequency of CRL/ARL publication is found in Section 4.4.5.1.

2.6.3 Access Controls

The DHS PKI shall protect any repository information not intended for public dissemination or modification. Public key certificates and certificate status information in the repository shall be publicly available. Where applicable, access privileges to information stored or controlled by a CA shall be determined by the DHS PKI PA.

2.6.4 Repositories

The DHS PKI shall include an X.500 master directory server system that is also accessible through the LDAP for repository services. The DHS PKI repository shall interoperate with the

FBCA repository and/or other Entity repositories, and contain the information necessary to support interoperation of the Entity PKI domains that employ the FBCA for this purpose.

The location of any repository shall be commensurate with the certificate using community, or one that provides access to Subscribers, Relying Parties, CAs, and RAs in accordance with the security requirements stipulated by this CP.

2.7 Compliance Audit

The DHS CAs and facilities shall have a compliance audit mechanism in place to ensure that the requirements of this CP, the associated CPS, and the provisions of the applicable MOAs are being implemented and enforced. The DHS PKI PA shall determine adequacy of the compliance audit reporting, and shall be responsible for ensuring all DHS CAs and Registration Authorities are audited for compliance on a periodic basis as set forth in Section 2.7.1.

2.7.1 Frequency of Entity Compliance Audit

The DHS CAs and RAs shall be subject to periodic compliance audits to validate that the PKI is operating in accordance with the security practices and procedures laid out in this CP, the applicable CPS, and any applicable MOAs. For High and Medium assurance CAs, the audit frequency shall be no less than one compliance audit per year. For Basic assurance CAs, the audit frequency shall be no less than one compliance audit every 2 years.

DHS CAs shall reserve the right to require periodic or aperiodic inspections or audits of any Subordinate CA or RA facility within the CA's domain to validate that the CA or RA is operating in accordance with the security practices and procedures laid out in the subordinate's CPS. The CA shall state the reason for any aperiodic inspection or audit.

The DHS PKI PA reserves the right to require an inspection or audit of any CA or RA asserting this policy, at any time. The DHS PKI PA also reserves the right to require an inspection or audit of any CSA operated to serve the DHS relying parties. The DHS PKI PA shall state the reason for any inspection or audit.

2.7.2 Identity/Qualifications of Compliance Auditor

The compliance auditor must perform CA or information system security compliance audits as its primary responsibility. The compliance auditor must be proficient in PKI technology and security auditing, and thoroughly familiar with this CP and all DHS PKI CPSs.

2.7.3 Compliance Auditor's Relationship to Audited Party

The compliance auditor either shall be independent from the DHS PKI, or it shall be sufficiently organizationally separated from DHS PKI to provide an unbiased, independent evaluation.

2.7.4 Topics Covered by Compliance Audit

The purpose of a compliance audit of the DHS PKI shall be to verify that all DHS CAs, CSAs, and RAs are complying with the requirements of this CP, the associated CPSs and MOAs. All aspects of entity operation as specified in this policy, the accompanying CPS and MOAs shall be subject to any compliance audit inspection.

2.7.5 Actions Taken as a Result of Deficiency

The DHS PKI PA may determine that a CA, CSA, or RA is not complying with its obligations, as set forth in this CP, or a respective CPS or MOA. Any discrepancies between a CA, CSA, or RA operation, and the stipulations of its CPS, MOA, and this CP shall be noted in an Audit Compliance Report. The DHS PKI PA shall determine an appropriate remedy that includes a time for completion.

Remedies may include permanent or temporary CA, CSA, or RA cessation, but several factors must be considered in this decision, including the severity of the discrepancy and the risks it imposes, and the disruption to the certificate using community. A special compliance audit may be required to confirm the implementation and effectiveness of the remedy.

2.7.6 Communication of Result

An Audit Compliance Report, including identification of corrective measures taken or being taken by the DHS OA shall be provided to the DHS PKI PA. Where appropriate, the DHS PKI PA shall notify subordinate or cross-certified CAs of the audit results. Details concerning who to notify and how the notification shall be made shall be documented in a signed Memorandum of Understanding (MOU) between the CAs.

2.8 Confidentiality

2.8.1 Types of Information to be Kept Confidential

A certificate shall only contain information that is relevant and necessary to effect secure transactions using the certificate. For the purpose of proper administration of the certificates, non-certificate information may be requested to manage the certificates (e.g., identifying numbers, business or home addresses and telephone numbers). Any such information shall be explicitly identified in a CPS. All personally identifiable information obtained from Subscribers in connection with the administration of the certificates shall be handled in accordance with the collection, maintenance, retention, and protection requirements of the Privacy Act of 1974.

Special procedures may be necessary to deal with aggregation of sensitive information within components of the infrastructure. Particular attention shall be paid to protect private (e.g., privacy act) information and information such as identification of law-enforcement personnel.

The following information shall also be considered confidential and may not be disclosed except as detailed in Sections 2.8.3 through 2.8.7:

- Audit trail records created and retained by the PKI
- Security measures of the PKI and its operation
- Disaster recovery plans

2.8.2 Types of Information Not Considered Confidential

To promote the interoperation and widespread utility of PKI resources, information included in certificates or the PKI repository (or any aggregation of that information) should be limited to information that is not overtly confidential. Certificates that are published to the PKI directory, or on a global repository are not considered confidential.

2.8.3 Disclosure of Certificate Revocation/Suspension Information

Information concerning the events leading up to, and the investigation of, a revocation shall be limited to those individuals with a need to know.

2.8.4 Release to Law Enforcement Officials

The DHS CAs may release sensitive information, including the private decryption key, in the course of a criminal investigation, as required by law. The DHS PKI is not obligated to inform the Subscriber of such release.

2.8.5 Release as Part of Civil Discovery

The DHS CAs shall release personally identifiable or other information submitted to the CA by a Subscriber if authorized by the Subscriber. Requests for releases of information that are not authorized by the Subscriber shall be referred to the DHS General Counsel for a determination to release or not to release. Non-disclosure of information shall remain an obligation notwithstanding the status of a certificate (current or revoked) or the status of the CA.

2.8.6 Disclosure Upon Owner's Request

Any personally identifiable information submitted to the CA by a Subscriber shall be made available to the Subscriber for individual review following an authenticated request by the Subscriber. This information shall be subject to correction and/or update at the Subscriber's request.

2.8.7 Other Information Release Circumstances

Audit trail information may only be released to the authorized auditing party, as determined by the DHS PKI PA.

2.9 Intellectual Property Rights

DHS shall maintain ownership of any public key certificates and private key that it issues, and any products or information developed under or pursuant to this CP. Because a Subscriber's private signature keys are created by the Subscriber and not issued by the DHS PKI, the Subscriber maintains ownership of the private signature keys.

3.0 IDENTIFICATION AND AUTHENTICATION

3.1 Initial Registration

3.1.1 Types of Names

DHS shall generate, sign, and process certificates that contain a X.500 Distinguished Name (DN) in the certificate subject name field. Certificates issued to CAs and RAs shall also use the X.500 DN form.

DHS certificates may additionally assert an alternate subject name, using the subjectAltName extension as defined in X.509, but it must be marked as non-critical.

3.1.2 Need for Names to be Meaningful

Subject DNs used within the DHS PKI shall uniquely identify the person or object that they are assigned to in a meaningful way. For people, this will typically be a legal name (e.g., Robert M. Smith). For devices, this may be a model name and serial number. For an application, the DNs will typically be the application name and specific module name.

Subscribers shall have DNs assigned to them by the CA or RA. The CA or RA shall determine a proper DN for a given Subscriber.

The CA asserting this policy shall only sign certificates with subject names from within a namespace approved by the DHS PKI PA. This constraint may be imposed through technical or procedural means.

3.1.3 Rules for Interpreting Various Name Forms

Rules for interpreting name forms shall be in accordance with the CAs certificate profile, defined in Section 7, in accordance with agency approved standards and guidelines.

Standards may include:

- X.500 for DN
- RFC-822 for Internet e-mail address
- Appropriate Internet RFCs for URL and IP address

3.1.4 Uniqueness of Names

Name uniqueness across the DHS PKI must be enforced.

Certificate subject name fields, including certificate subject and subject alternate name, must be unique for each certificate issued within the X.500 name space of the domain of the Root CA. The CA(s) and RAs shall enforce name uniqueness.

3.1.5 Name Claim Dispute Resolution Procedure

The DHS PKI PA shall investigate and correct any name duplication brought to its attention. The DHS PKI PA is the final arbiter in name dispute resolution (when the CA is unable to resolve a dispute) and reserves the right to reject any name at its sole and absolute discretion.

3.1.6 Recognition, Authentication and Role of Trademarks

No stipulation.

3.1.7 Method to Prove Possession of Private Key

In all cases where the applicant Subscriber generates keys, the applicant Subscriber is required to prove possession of the private key, which corresponds to the public key in the certificate issuance request.

For Rudimentary and Basic assurance certificates, the Subscriber's signature keys shall be generated directly by the Subscriber in either software or hardware, or in a key generator that benignly transfers the key to the Subscriber.

For Medium and High assurance certificates, the Subscriber's signature keys shall be generated directly by the Subscriber on a token, or in a key generator that benignly transfers the key to the Subscriber's token.

For key management keys, if the CA generates the key management keys, the token shall be delivered to the end-entity via a secure and accountable method. The DHS PKI PA may allow other mechanisms for key management keys that are at least as secure as those cited here.

For all assurance levels, when keyed hardware tokens are delivered to certificate subjects, the delivery shall be accomplished in a way that ensures that the correct tokens and activation data are provided to the correct subjects. The DHS CA must maintain a record of validation for receipt of the token by the subject. When any mechanism that includes a shared secret (e.g., a password or PIN) is used, the mechanism shall ensure that the applicant and the DHS CA are the only recipients of this shared secret.

3.1.8 Authentication of Organization Identity

Requests for certificates in the name of an organization shall require authentication of that organization's identity.

For organizations external to DHS, organization identification information shall include the organization name, address, and documentation of the existence of the organization. The DHS OA shall verify the organization identity information, verify the identity information of the requesting representative of the organization in accordance with authentication of individual identity as in Section 3.1.9, and verify the authority of the requestor to act in the name of the organization.

For DHS organizations and sub-organizations, organization identification information shall include the organization name. The Registrar shall verify the organization identity information, verify the identity information of the requestor in accordance with authentication of individual identity as defined in Section 3.1.9, and verify the authority of the requestor to act in the name of the organization.

The applicable CPS shall determine the usage of other types of organizational certificates. If the CPS permits the use of organizational certificates, identity authentication shall be carried out in accordance with this section.

3.1.9 Authentication of Individual Identity

For individuals requesting a DHS PKI certificate, the CA shall ensure that the applicant's identity information is verified and checked in accordance with this CP and the applicable CPS. The CA shall ensure that the applicant's identity and public key are properly bound. The authentication process shall involve an applicant presenting acceptable identification credentials to the Registrar (RA, LRA or TA) personnel. The Registrar personnel shall record the process that was followed for each identity authentication and each certificate issuance.

The process information to record includes:

- The identity of the person performing the identification
- A signed declaration by that person that he or she verified the identity of the applicant, including verification of any roles or authorizations that apply to the certificate

- An employee number or a unique identifying number from the ID of both participants (the verifier and the applicant)
- The date and time of the verification
- A declaration of identity signed by the applicant

The following guidelines are provided to establish the identification requirements for the registration process.

3.1.9.1 Rudimentary Assurance

For Rudimentary assurance certificates, there is no authentication required. Applicants may request and obtain a certificate by providing a valid email address.

3.1.9.2 Basic Assurance

The basis of establishing identity for Basic assurance certificates is through an association with a service, agency, or other component of the DHS. This association may be established by any of the following:

- In-person proofing before the appropriate Registrar personnel
- Through comparison of applicant supplied information with information in a trusted database
- Attestation of a supervisor, or administrative or information security officer, or a person certified by DHS as being authorized to confirm identities (such as notaries public) who uses a stamp, seal or other mechanism to authenticate their identity confirmation

There is no requirement to demonstrate a particular need for the certificate.

3.1.9.3 Medium Assurance

For Medium assurance certificates, the applicant must appear personally before the appropriate Registrar personnel or before an entity certified by a State or Federal Agency as being authorized to confirm identities (such as notaries public) who uses a stamp, seal or other mechanism to authenticate their identity confirmation. The information provided must be verified to ensure legitimacy.

The credentials required are either of the following:

- One Federal Government-issued picture ID (e.g., a passport)
- Two Non-Federal Government IDs, one of which shall be a picture ID (e.g., Drivers License)

The applicant must identify a need for the certificate, as described in the applicable CPS.

3.1.9.4 High Assurance

For High assurance certificates, the applicant must appear personally before the appropriate Registrar personnel and present appropriate, verifiable credentials. The information provided must be verified to ensure legitimacy.

The credentials required are either of the following:

- One Federal government-issued picture ID (e.g., passport)

- Two Non-Federal government IDs, one of which shall be a picture ID (e.g., drivers license)
 The applicant must identify a need for the certificate, as described in the applicable CPS.

3.1.9.5 For All Levels:

If an Applicant is unable to perform face-to-face registration alone (e.g., a network device), the applicant shall be represented by a trusted person already issued a digital certificate by the Entity. The trusted person will present information sufficient for registration at the level of the certificate being requested, for both himself/herself and the applicant who the trusted person is representing.

Exhibit 3 summarizes the identification requirements for each level of assurance:

Exhibit 3: Identification Requirements

Assurance Level	Identification Requirements
Test	No stipulation.
Rudimentary	No identification requirement; applicant may apply and receive a certificate by providing his or her e-mail address.
Basic	Identity may be established by in-person proofing before a Registrar; or comparison with trusted information in a data base of user-supplied information (obtained and/or checked electronically, through other trusted means such as the U.S. mail or in-person); or by attestation of a supervisor, or administrative or information security officer, or a person certified by a state or Federal Agency as being authorized to confirm identities.
Medium	Identity shall be established by in-person proofing before the Registration Authority, Trusted Agent or an entity certified by a State or Federal Entity as being authorized to confirm identities; information provided shall be verified to ensure legitimacy. A trust relationship between the Trusted Agent and the applicant which is based on an in-person antecedent may suffice as meeting the in-person identity proofing requirement. Credentials required are either one Federal Government-issued Picture I.D., or two Non-Federal Government I.D.s, one of which shall be a photo I.D. (e.g., Drivers License)
High	Identity established by in-person appearance before a Registrar; information provided shall be checked to ensure legitimacy. Credentials required are either one Federal government-issued picture ID, or two non-Federal government IDs, one of which shall be a photo ID (e.g., drivers license).

3.1.10 Authentication of Component Identities

Some computing and communications components (routers, firewalls, servers, CSA, etc.) may be named as certificate subjects. In such cases, the component Subscriber shall have a human sponsor. The human sponsor shall provide credentials in accordance with the requirements of Section 3.1.9 during authentication on behalf of the component Subscriber.

Additionally, the human sponsor shall provide appropriate component authentication information consisting of the following items (at a minimum):

- Component identification (e.g., serial number) or service name (e.g., DNS name)
- Component attributes to be included in the certificates
- Component public keys
- Sponsor contact information

The registration information shall be verified to an assurance level commensurate with the certificate assurance level being requested. Acceptable methods for performing this authentication and integrity checking include, but are not limited to:

- Verification of digitally signed messages sent from the sponsor (using certificates of equivalent or greater assurance than that being requested)
- In person registration by the sponsor, with the identity of the sponsor confirmed in accordance with the requirements of Section 3.1.9

3.2 Routine Re-key, Certificate Renewal, and Update

The longer and more often a key is used, the more susceptible it is to loss or discovery. Therefore, it is important that Subscribers periodically obtain new keys and re-establish their identity.

Subscribers of DHS CAs shall identify themselves for the purpose of re-keying or renewing a certificate as required in Exhibit 4:

Exhibit 4: Routine Re-key and Certificate Renewal Identity Requirements for Subscriber Signature and Encryption Certificates

Assurance Level	Routine Re-key and Certificate Renewal Identity Requirements for Subscriber Signature and Encryption Certificates
Test	No Stipulation.
Rudimentary	Identity may be established through use of current signature key.
Basic	Identity may be established through use of current signature key, except that identity shall be reestablished through initial registration process at least once every 15 years from the time of initial registration, as described in Section 3.1.9.
Medium	Identity may be established through use of current signature key, except that identity shall be established through initial registration process at least once every 9 years from the time of initial registration, as described in Section 3.1.9.
High	Identity may be established through use of current signature key, except that identity shall be established through initial registration process at least once every 3 years from the time of initial registration, as described in Section 3.1.9.

3.3 Obtaining a New Certificate After Revocation

After a certificate has been revoked for reasons other than during a renewal or update action, the Subscriber must go through the initial registration process described in Section 3.1 to obtain a new certificate.

3.4 Revocation Request

All revocation requests, whether communicated in writing or submitted electronically, shall be authenticated by a trustworthy means. Revocation requests authenticated on the basis of the key pair being revoked (whether or not compromised) shall always be accepted as valid.

The Registrars shall permit Subscribers, or another person authorized to act on behalf of the Subscriber, to request revocation of a DHS issued certificate in which the Subscriber is identified as the Subject in the certificate. The Registrars may request revocation of certificates of Subscribers in the event of a private key compromise or when they are no longer authorized Subscribers (e.g., change of employment or for other administrative reasons).

4.0 OPERATIONAL REQUIREMENTS

4.1 Application for a Certificate

4.1.1 Cross-Certification Certificate Application

Requests by a non-DHS Certification Authority for cross certification with a DHS Certification Authority shall be submitted to the DHS PKI PA using the contact information provided in Section 1.5.2. The submission shall include the CP and CPS for the CA, written to the format of the *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework* [IETF RFC2527]. The request shall also propose a mapping between the levels of assurance expressed in the submitted CP and those in the DHS CP.

If the DHS PKI PA determines that DHS is interested in cross certification with the requesting entity's CA, the DHS PKI Operational Authority will compare the submitted CP and CPS against the DHS CP, and submit its findings to the DHS PKI PA. If the DHS PKI PA determines that the submitted CP and CPS are acceptable, the requesting entity will then be required to demonstrate interoperability with the DHS CA via tests performed under the direction of the DHS PKI OA. The DHS PKI PA may also require an initial compliance audit, performed by parties of the DHS PKI PA's choosing, to ensure that the CA is prepared to implement all aspects of the submitted CP and CPS.

If the submitted CP and CPS evaluation, interoperability testing and compliance audit are acceptable, the DHS PKI PA will execute a Memorandum of Agreement between the DHS and the requesting entity, that sets forth the respective responsibilities and obligations of both parties, and the mappings between the certificate levels of assurance contained in this CP and those in the submitted CP. Upon the successful completion of these steps, the DHS PKI PA shall authorize cross-certification with the non-DHS CA.

4.1.2 Subordinate CA Certificate Application

As part of the initial DHS Root and Subordinate CA Key Generation Ceremonies, a certificate was issued to a single DHS medium level of assurance Subordinate Certification Authority (CA). Subsequent DHS CAs added to the DHS PKI will be subordinate to the DHS Root CA.

The following is the process to add Subordinate DHS CAs to the DHS PKI:

- The DHS Sponsor of the proposed CA must complete and sign a request to add the CA as a Subordinate CA under the DHS Root CA. The request must include a justification for adding the Subordinate CA to the DHS PKI
- The following documentation must be submitted with the request:
 - The Certification Practices Statement (CPS) for the Subordinate CA written to the format of the *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework* [IETF RFC2527]. If Online Certificate Status Processing is to be used, the Certification Practices Statement (CPS) must address the practices followed by the Certificate Status Authority (CSA)
 - A proposed mapping between the level(s) of assurance expressed in the submitted CPS and those in the DHS CP
 - A detailed description of the registration process for the Subordinate CA
 - Documentation of the engineering design for the Subordinate CA and its components, including all of the hardware and software products used, and configurations
 - The plan for integrating/interfaces the Directory and other key components used by the Subordinate CA with their counterparts used by the existing DHS PKI
 - The proposed Subordinate CA Key Generation Ceremony (KGC) Script

The DHS PKI PA may decide to deny the request or to proceed with the process to add the Subordinate CA. The DHS PKI PA notifies the DHS PKI OA and the Sponsor, in writing, of the decision. If the DHS PKI PA decides to proceed with the process to add the Subordinate CA to the DHS PKI, the DHS PKI PA completes the following:

- Tasks the DHS PKI Auditor to conduct a Compliance Review consisting of:
 - Mapping the Subordinate CA CPS to the DHS CP
 - Reviewing the proposed Key Generation Ceremony for compliance with the Subordinate CA CPS and best practices
- Establishes a Subordinate CA Review Group, chaired by the DHS PKI PA or the DHS PKI OA, and staffed by the DHS PKI Security Compliance Officer, knowledgeable engineering and policy personnel from the existing staff of the DHS PKI and Office of the Chief Information Security Officer, and non-voting personnel representing the proposed Subordinate CA to:
 - Review the submitted documentation for security, interface and interoperability issues
 - Review the results of the Compliance Review by the DHS PKI Auditor

- Work with appropriate representatives of the Subordinate CA to resolve issues
- Work with appropriate representatives of the Subordinate CA to modify the Subordinate CA's Certificate Practices Statement (CPS) to address Auditor findings and resolve issues
- When appropriate, recommend approval by the DHS PKI Policy Authority, noting any unresolved issues

The DHS PKI PA approves the addition of the Subordinate CA by signing the version of the Subordinate CA's Certificate Practices Statement recommended by the Subordinate CA Review Group. Once the CPS has been signed, the DHS PKI OA oversees the completion of the following by the DHS PKI staff and Subordinate CA staff:

- Performing the Subordinate CA Key Generation Ceremony, including signing of the Subordinate CA Certificate by the DHS Root CA. An Auditor, who is knowledgeable of PKI, and approved by the DHS PKI PA, must witness the Key Generation Ceremony and submit a Key Generation Ceremony Report to the DHS PKI PA.
- Conducting interoperability testing with the existing DHS PKI, and resolving any problems encountered
- Obtaining DHS Certification & Accreditation of the Subordinate CA

Once these steps have been completed the Subordinate CA may commence operations.

The DHS PKI PA will ensure that the DHS PKI Auditor conducts an initial Compliance Audit of the Subordinate CA within 6 months of initial operations. Compliance Audits are described in Section 2.7.

4.1.3 Subscriber Certificate Application

The Subscriber applicant and the Registrar shall perform the following steps when a Subscriber applies for a certificate:

- Determine that the Subscriber applicant is authorized to be issued certificates (in accordance with this Policy and the applicable CPS)
- Establish and record the identity of Subscriber (per Section 3.1)
- Obtain a functioning public/private key pair for each certificate required and prove that the private key is held by the Subscriber (per Section 3.1.7)
- Provide a point of contact for verification of any roles or authorizations requested

These steps may be performed in any order that is convenient for the CA and users, as long as this does not defeat security. However, all of these steps must be completed prior to certificate issuance.

Any electronic transmission of shared secrets communicated during the certificate application process shall be protected (e.g., encrypted) using means commensurate with the requirements of the data to be protected by the certificates being issued.

Identity proofing shall be done between the Subscriber applicant (or Sponsor in the case of device certificates) and the Registrar as required by this Policy (per Sections 3.1.8, 3.1.9, and

3.1.10). All certificate applicants shall provide a completed Subscriber Agreement to the RA or LRA.

The DHS CAs implementing this Policy shall not certify other CAs (to include cross-certification) unless authorized by the DHS PKI PA to do so, and then may only do so within any constraints imposed by the DHS PKI PA.

4.1.4 Delivery of Public Key for Certificate Issuance

For all key pairs generated by the Subscriber applicant (or Registrar), the public key shall be delivered to the CA in a way that binds the Subscriber applicant's verified identification to the public key. This binding shall be accomplished using means that are as secure as the security services being offered by the keys being certified. The binding shall be accomplished using cryptographic, physical, procedural, and any other appropriate methods. For public keys to be issued in High Assurance certificates, the binding must be accomplished using cryptography. When cryptography is used, it must be at least as strong as that employed in certificate issuance. The methods used for delivery are stipulated in the CPS.

In cases where key pairs (other than signature keys) are generated by the CA or Registrar on behalf of the Subscriber, the CA or Registrar shall implement secure mechanisms to ensure that the hardware or software token that holds the public/private key pair is securely sent to the proper Subscriber, and that this token is not activated by an unauthorized entity.

4.2 Certificate Issuance

Certificates shall be generated based on Registrar review and approval of the Certificate Application and submission of a certificate request to the CA. A Registrar may accept and review the certificate request, but the CA shall ultimately approve the certificate request, and the CA shall sign and issue the certificate. The Registrar may submit the certificate request on behalf of the Subscriber applicant. The certificate request may be submitted and processed electronically.

While the Subscriber applicant may do most of the data entry, it is still the responsibility of the Registrar to verify that the information is correct and accurate. This may be accomplished through a system approach linking trusted databases containing personnel information, other equivalent authenticated mechanisms, or through personal contact with the Subscriber. If databases are used to confirm Subscriber applicant information, then these databases must be protected from unauthorized modification to a level commensurate with the level of assurance of the certificate being sought.

Upon receiving the certificate request, the CA shall:

- Verify the identity of the requestor
- Verify the authority of the requestor and the integrity of the information in the certificate request
- Build and sign a certificate, if all certificate requirements have been met (or sign the certificate that is built by a Registrar or Subscriber)
- Make the certificate available to the Subscriber, and post it to a repository

To the extent practical, certificates once created shall be checked to ensure that all fields and extensions are properly populated. This may be done through software that scans the fields and extensions looking for any evidence that a certificate was improperly manufactured.

4.2.1 Delivery of Subscriber's Private Key to Subscriber

For signature keys, the key pair shall be generated by the Subscriber, or in the Subscriber's presence, and shall remain within the cryptographic boundary of the Subscriber's cryptographic module. Therefore, there is no delivery of the private signature key. Under no circumstances shall anyone other than the Subscriber have possession or knowledge of the private signature key.

In cases where key pairs (other than signature keys) are generated by the CA or Registrar, the module must be delivered to the Subscriber in a secure manner. This delivery shall be accomplished using means that are as secure as the security services offered by the keys being certified. Accountability for the location and state of the module must be maintained until the Subscriber accepts possession. The Subscriber shall acknowledge receipt of the module.

Normally a certificate shall be issued to a single Subscriber. For cases where there are several entities acting in one capacity, and where non-repudiation for transactions is not desired, a certificate may be issued that corresponds to a private key that is shared by multiple Subscribers. In these cases:

- An Information Systems Security Officer or equivalent shall be responsible for ensuring control of the private key, including maintaining a list of Subscribers who have access to use of the private key, and accounting for which Subscriber had control of the key at what time
- The subjectName DN must not imply that the subject is a single individual, e.g., by inclusion of a human name form
- The list of those holding the shared private key must be provided to, and retained by, the applicable CA or its designated representative
- The procedures for issuing tokens for use in shared key applications must comply with all other stipulations of this CP (e.g., key generation, private key protection, and Subscriber obligations)

4.2.2 CA Public Key Delivery

The public key of the Root CA must be available, in its self-signed public certificate form, for certificate trust paths to be created and verified. The CA certificate must be delivered in a secure manner.

4.3 Certificate Acceptance

Acceptance is the action taken by a Subscriber that triggers the Subscriber's duties and potential liability following the issuance of a certificate. It is the responsibility of the CA or Registrar through the delivery process to:

- Explain to the Subscriber their responsibilities
- Inform the Subscriber of the creation of a certificate and to the contents and purpose of the certificate

- For High and Medium Assurance certificates, require the Subscriber to sign documentation indicating acceptance of their responsibilities (as defined in Section 2.1.3)
- For any certificates issued with an assurance level less than Medium, require the Subscriber to indicate acceptance of their responsibilities (as defined in Section 2.1.3)—signature is not required

The certificate acceptance process is complete when the Subscriber (or surrogate) accomplishes a technical or procedural mechanism, specified in the CPS, to indicate acceptance of their certificate.

4.4 Certificate Revocation and Suspension

Certificates have one of three states during their validity period (after issuance and before expiration): active, inactive, or revoked.

Certificates in an active state are ready and able to be used for their intended functions.

Certificates that are inactive are temporarily invalid, denying all privileges to the Subscriber. Subscribers presenting an inactive certificate are denied access that the certificate would normally allow. Inactive certificates can be reactivated, prior to expiration, to return their privileges.

The inactive period must be no longer than 90 days. Certificates that have been inactive for more than 90 days shall be revoked.

Certificates that have been revoked are made permanently invalid removing all privileges to the Subscriber. Subscribers presenting a revoked certificate are denied access that the certificate would normally allow. Revoked certificates cannot be reinstated. Revoked certificates are published on the CRL.

4.4.1 Circumstances for Revocation or Suspension

A certificate shall be revoked when the binding between the Subject and the Subject's public key contained within a certificate is no longer considered valid. Examples of circumstances that invalidate the binding include:

- Identifying information in the certificate becomes invalid
- The Subscriber or CA, in cases of cross-certification, can be shown to have violated, or are suspected of violating the Subscriber Agreement, the requirements set forth by this CP, the applicable CPS, or the MOA
- The Subscriber's or CA's private keys have been or are suspected of having been compromised. This includes private keys being lost, stolen, or destroyed in a fashion where there is potential for compromise or loss of control
- The Subscriber, CA, or other authorized party (as defined in the applicable CPS) asks for their/its certificate to be revoked
- A Subscriber ceasing its relationship with DHS, prior to departure, surrenders to the organization (through any accountable mechanism) all cryptographic hardware tokens that were issued by or on behalf of DHS

- If a Subscriber leaves an organization and the hardware tokens cannot be obtained from said Subscriber, then all certificates associated with the un-retrieved tokens shall be immediately revoked. The reason code “key compromise” shall be asserted in this situation

Whenever any of the above circumstances occur, the associated certificate shall be revoked and placed on the ARL/CRL. Revoked certificates shall be included on all new publications of the ARL/CRL until the certificates expire.

The applicable CPS may specify circumstances that do not invalidate the binding between the certificate subject and public key, but do require certificate deactivation. Certificate deactivation shall not be used as an alternative to revocation. A certificate shall not be inactive for any of the revocation reasons previously given.

4.4.2 Who Can Request Revocation or Suspension

Within the DHS PKI, a CA may summarily deactivate or revoke certificates within its domain. A written notice and brief explanation for the revocation shall subsequently be provided to the Subscriber.

A Registrar can request the deactivation or revocation of a Subscriber’s certificate on behalf of any authorized party as specified in the CPS.

A Subscriber may request the deactivation or revocation of its own certificate.

4.4.3 Procedure for Revocation or Suspension Request

A Subscriber or other authorized individual may request deactivation or revocation of a certificate electronically, in writing, or by telephone to a Registrar by way of a certificate deactivation/revocation request.

If the request is made electronically, the individual submitting the request shall digitally sign the request.

The Subscriber or other authorized individual can make a written request by sending an inked signature message requesting deactivation or revocation to the CA.

For telephone requests, the Registrar accepting the request shall retain a written record of the call to aid in processing the request. The CA shall require identity authentication of the requestor.

If a Subscriber is requesting the deactivation or revocation of his or her own certificate, any of the three previous methods may be utilized by dividing the process into two steps. The first step is the Subscriber presenting the request to a Registrar, and the second step is the Registrar presenting the request to the CA. The Registrar may have the ability to execute the request and complete the deactivation or revocation with the CA, without participation from CA personnel.

If an authorized individual requests deactivation or revocation of a Subscriber’s certificate other than their own, the identity of the authorized party must be authenticated to a Registrar, as that Registrar will make the request to the CA on behalf of the authorized party.

For example, a Subscriber’s supervisor may present a request for deactivation or revocation of that Subscriber’s certificate to a Registrar. The Registrar will determine the validity of the request, and may then make the deactivation or revocation request to the CA. In such cases, the Registrar must authenticate the identity of the Subscriber’s supervisor making the request.

All requests to deactivate or revoke a certificate shall identify the certificate to be revoked, explain the reason for revocation, and allow the identity of the requestor to be authenticated.

If the Subscriber is using hardware tokens for key storage, the Subscriber shall, prior to departure, surrender to DHS all cryptographic hardware tokens that were issued by or on behalf of DHS. The tokens shall be zeroized or destroyed promptly upon surrender and shall be protected from malicious use between surrender and zeroization or destruction. If the hardware tokens cannot be obtained from the Subscriber, then all Subscriber's certificates associated with the non-recovered tokens shall be immediately revoked for the reason of key compromise.

4.4.4 Revocation Request Grace Period

There is no revocation grace period for the Subscribers. Subscribers and other authorized individuals shall request revocation of a certificate as soon as they recognize the need for revocation, as specified in Section 4.4.1.

4.4.5 Certificate Revocation Lists

All DHS PKI CAs shall issue CRLs. CRLs are lists of revoked certificates, digitally signed by the associated CA, and posted for relying parties to verify the validity of certificates. If the CA software lists revoked CA certificates separately, in CRLs specifically for CA certificates (ARLs), these ARLs shall also be issued by such CAs. To the extent practical, the contents of ARLs and CRLs shall be checked before issuance to ensure that all information is correct. This may be done using software which scans the ARLs and CRLs looking for any evidence of an improperly manufactured ARL or CRL.

4.4.5.1 CRL Issuance Frequency

CRLs shall be issued periodically, even if there are no changes to be made, to ensure timeliness of information.

The DHS PKI Offline Root CA shall issue and publish CRLs (including ARLs) upon each update (revocation) and at least once per month. All other DHS PKI CAs shall issue and publish CRLs (including ARLs) upon each update (revocation) and at least once per day.

If the CRL is being issued as a result of a compromise of a Medium or High assurance certificate, it shall be posted as quickly as feasible, and at least within 6 hours of notification of the compromise.

CRLs shall be published not later than the next scheduled update.

4.4.6 CRL Checking Requirements

Use of revoked certificates could have damaging or catastrophic consequences. Relying parties are required to perform certificate status checking, to obtain any assurance with a DHS PKI certificate. The matter of how often new revocation data should be obtained is a determination to be made by the relying party. If it is infeasible to obtain current revocation information, then the relying party should reject use of the certificate because the certificate's authenticity cannot be guaranteed to the standards of this policy.

4.4.7 Online Revocation Status Checking

Online status checking may optionally be supported. Clients using on-line status checking will not need to obtain or process CRLs.

Online DHS CSAs used for verifying certification paths (e.g., SCVP Server) shall ensure that:

- Certificates indicated as being valid have a chain of valid certificates (valid as defined by the X.509 standard) linking back to a DHS PKI PA approved “trusted CA”
- Each certificate in the certificate chain used to validate the certificate whose status is being requested is checked for revocation, such that the Relying Party need not check more than one CSA to validate a Subscriber certificate
- Certificate status responses provide authentication and integrity services commensurate with the assurance level of the certificate being verified
- It is made clear in the certificate status response, which attributes, if any, other than certificate subject name (e.g., citizenship, clearance authorizations, etc.) are being authenticated by the CSA

Online CSAs that provide revocation status information only (e.g., OCSP Responder) shall ensure that:

- Accurate and up-to-date information from the authorized CA is used to provide the revocation status
- Revocation status responses provide authentication and integrity services commensurate with the assurance level of the certificate being checked

DHS relying parties that use certificate status information from CSAs not approved by the DHS PKI PA do so at their own risk.

4.4.8 Other Forms of Revocation Checking

Any alternate forms used to disseminate revocation information shall be implemented in a manner consistent with the security requirements for the implementation of CRLs and on-line revocation and status checking.

4.5 Security Audit Procedure

Audit log files shall be generated for all events relating to the security of the DHS CAs. Where possible, the security audit logs shall be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism shall be used. All security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits. The security audit logs for each auditable event defined in this section shall be maintained in accordance with the retention period for archive as specified in Section 4.6.2.

4.5.1 Types of Events Recorded

The PKI equipment shall be able to record events related to the server (installation, modification, accesses), and the application (requests, responses, actions, publications, and error conditions). Events may be attributable to human action or automatically invoked by the equipment.

At a minimum, the information recorded shall include:

- Type of event
- Entities involved
- Date and time the event occurred
- Success or failure of the event/attempt

In addition, for some types it will be appropriate to record the following:

- The source and destination of a message (CSAs are exempt from this audit requirement)
- The disposition of a created object (e.g., a filename)

A message from any source requesting an action by a DHS CA is an auditable event (i.e., certificate requests, revocation requests, creation of certificates, generation and posting of CRLs, etc.). The message must include message date and time, source, destination and contents. The CA's CPS shall identify each of the audit events for the CA.

The auditing capabilities of the underlying equipment operating system shall be enabled during installation. A record shall be kept of file manipulation and account management. These events shall also be recorded during normal operation of the PKI equipment.

Exhibit 5 identifies the minimum audit events that shall be recorded for the PKI. These events may be recorded electronically by the operating system on the CA or Directory servers, the CA application software or manually by a trusted role.

Exhibit 5: Auditable Events

Event Category	Event Description
Security Audit	Any changes to the Audit parameters, e.g., audit frequency, type of event audited
	Any attempt to delete or modify the Audit logs
Identification and Authentication	Successful and unsuccessful attempts to assume a role
	Change in the value of maximum authentication attempts
	Maximum number of unsuccessful authentication attempts during user login
	An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts
	An Administrator changes the type of authenticator, e.g., from password to biometrics
Key Generation	Whenever the CA generates a key. (Not mandatory for single session or one-time use symmetric keys)
Private Key Load and Storage	The loading of Component private keys
	All access to certificate subject private keys retained within the CA for key recovery purposes

Event Category	Event Description
Trusted Public Key Entry, Deletion and Storage	All changes to the trusted public keys, including additions and deletions
Private Key Export	The export of private keys (keys used for a single session or message are excluded)
Certificate Registration	All certificate requests
Certificate Revocation	All certificate revocation requests
Certificate Status Change	The approval or rejection of a certificate status change (i.e., from "Valid" to "Revoked," etc.)
Ca Configuration	Any security-relevant changes to the configuration of the CA
Account Administration	Roles and users are added or deleted
	Access control privileges of a user account or a role are modified
Certificate Profile Management	All changes to the certificate profile
Certificate Revocation List Profile Management	All changes to the certificate revocation list profile
Miscellaneous	Installation of the Operating System
	Installation of the CA
	Installing hardware cryptographic modules
	Removing hardware cryptographic modules
	Destruction of cryptographic modules
	System Startup
	Logon Attempts to CA applications
	Receipt of Hardware/Software
	Attempts to set passwords
	Attempts to modify passwords
	Backing up CA internal database
	Restoring CA internal database
	File manipulation (e.g., creation, renaming, moving)
	Posting of any material to a repository
	Access to CA internal database
	All certificate compromise notification requests
	Loading tokens with certificates
	Shipment of Tokens
Zeroizing tokens	
Re-key of the CA	

Event Category	Event Description
	Configuration changes to the CA server involving: <ul style="list-style-type: none"> • Hardware • Software • Operating System • Patches • Security Profiles
Physical Access/Site Security	Personnel Access to room housing CA
	Access to the CA server
	Known or suspected violations of physical security
Anomalies	Software Error conditions
	Software check integrity failures
	Receipt of improper messages
	Misrouted messages
	Network attacks (suspected or confirmed)
	Equipment failure
	Electrical power outages
	Uninterruptible Power Supply (UPS) failure
	Obvious and significant network service or access failures
	Violations of Certificate Policy
	Violations of Certification Practice Statement
	Resetting Operating System clock

4.5.2 Frequency of Processing Data

All CA audit logs shall be periodically reviewed in accordance with the schedule specified in the applicable CPS, but shall meet at a minimum the schedule shown in Exhibit 6.

Exhibit 6: Audit Log Review Schedule

Assurance Level	Review Audit Log
Test	No Stipulation
Rudimentary	Only required for cause
Basic	Only required for cause
Medium	At least once every 2 months
High	At least once per month

Security audit data shall be reviewed periodically. At a minimum, a statistically significant set of security audit data generated by the CAs since the last review shall be examined, as well as a reasonable search for any evidence of malicious activity. The OA shall explain all significant events in an audit log summary.

At a minimum, review shall involve verifying that the log has not been tampered with, and then briefly inspecting all log entries, with a more thorough investigation of any logged alerts or irregularities that might have an impact on the overall security and/or trustworthiness of the PKI. Actions taken as a result of these reviews shall be documented.

4.5.3 Retention Period for Audit Log

Audit logs shall be retained onsite for at least 2 months. The information generated on the PKI equipment shall be kept on the PKI equipment until the information is moved to an appropriate archive facility.

4.5.4 Protection of Audit Log

The audit log, to the extent possible, shall not be open for read or modification by any human, or by any automated process other than those authorized to perform audit processing. No entity that has modification access to the audit log may archive it. (Note: Deletion requires modification access.) Only authorized personnel may archive audit logs. Audit data generated in hardcopy shall be copied and stored in a safe, secure storage location separate from the PKI equipment.

The individual who removes audit logs from the CA systems shall not be capable of directly or indirectly activating or using the CA signature key.

4.5.5 Audit Log Backup Procedures

The audit logs generated on the PKI equipment may be backed up on the same schedule as the rest of the data on the PKI equipment, but at a minimum must be backed up at least once per month. Audit log backups shall be moved at least once per month to a safe, secure storage location separate from the PKI equipment.

4.5.6 Audit Collection System (Internal vs. External)

There is no requirement for the audit log collection system to be external to the PKI equipment. Audit processes shall be invoked at system startup, and cease only at system shutdown. Should it become apparent that an automated audit system has failed, the PKI operation shall cease until the audit capability can be restored.

4.5.7 Notification to Event-Causing Subject

This CP imposes no requirement to provide notice that an event was audited to the individual, organization, device, or application that caused the event. Real-time alerts are neither required nor prohibited by this policy.

4.5.8 Vulnerability Assessments

The DHS OA shall perform routine self-assessments of security controls.

The OA, including those personnel operating the CAs shall be watchful for attempts to violate the integrity of the PKI system, including the equipment, physical location, and personnel. The audit logs shall be checked for anomalies in support of any suspected violation. The audit logs shall be reviewed by the PKI Auditor for events such as repeated failed actions, requests for privileged information, attempted access of system files, and unauthenticated responses. PKI Auditors shall also check for continuity of the audit logs.

4.6 Records Archival

4.6.1 Types of Events Archived

PKI archive records shall be sufficiently detailed so that they can be used to establish the proper operation of the CA or the validity of any certificate (including those revoked or expired) issued by the CA. At a minimum, the following data shall be archived (CA and certificate data archive requirements refer only to data associated with operational CAs).

The following data shall be recorded for archive at the initialization of the PKI equipment:

- PKI system equipment configuration files
- PKI Accreditation
- Completed CP and CPS
- Contractual Obligations

At a minimum, the data listed in Exhibit 7 shall be recorded for archive in accordance with each assurance level (not applicable to Test Assurance).

Exhibit 7: Archive Requirements

Data To Be Archived	Rudimentary	Basic	Medium	High
DHS CA accreditation (if applicable)	X	X	X	X
Certification Practice Statement	X	X	X	X
Contractual obligations	X	X	X	X
System and equipment configuration	X	X	X	X
Modifications and updates to system or configuration	X	X	X	X
Certificate requests	X	X	X	X
Revocation requests		X	X	X
Subscriber identity Authentication data as described in Section 3.1.9		X	X	X
Documentation of receipt and acceptance of certificates		X	X	X
Documentation of receipt of tokens		X	X	X
All certificates issued or published	X	X	X	X
Record of DHS CA and CSA Re-key	X	X	X	X
All ARLs and CRLs issued and/or published		X	X	X
All Audit Logs	X	X	X	X
Other data or applications to verify archive contents		X	X	X
Documentation required by compliance auditors		X	X	X

4.6.2 Retention Period for Archive

All sensitive events, lists, certificates, keys, records, reports, agreements and correspondence archived shall be retained in accordance with the retention schedule and procedures specified in the CPS. The minimum retention periods for archive data is listed in Exhibit 8.

Exhibit 8: Archive Retention Schedule

CA Assurance Level	Retention Period
High	20 years and 6 months
Medium	10 years and 6 months
Basic	7 years and 6 months
Rudimentary	7 years and 6 month
Test	No Stipulation

If the original archive media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media shall be defined by the archive site. Applications required for viewing archive records must be maintained for at least the applicable retention period.

Prior to the end of the archive retention period, DHS shall provide archived data and the applications necessary to read the archives to an approved archival facility, which shall retain the applications necessary to read this archived data.

4.6.3 Protection of Archive

No unauthorized user shall be able to read, write to, modify, or delete the archive. However, archived records may be moved to another medium when authorized by the DHS PKI PA. The contents of the archive shall not be released as a whole, except as required by law. Records of individual transactions may be released upon request of any Subscribers involved in the transaction or their legally recognized agents.

Archive records shall be labeled with the CA's name, archive contents, the date, and any appropriate data-classification label.

Archive media shall be stored in a separate, safe, secure storage facility.

4.6.4 Archive Backup Procedures

No stipulation.

4.6.5 Requirements for Time Stamping of Records

No stipulation.

4.6.6 Archive Collection System (Internal and External)

No stipulation.

4.6.7 Procedures to Obtain and Verify Archive Information

Procedures detailing how to create, package, and send the archive information shall be published in the CA's CPS. Only authorized users shall be allowed to access the archive.

4.7 Key Changeover

4.7.1 Certificate Re-key

Re-keying a certificate means that a new certificate is created that has the same characteristics and assurance level as the old one. However, the new certificate has a new, different public key (corresponding to a new, different private key); a different serial number; and is assigned a different validity period.

To minimize risk from compromise of a CA's private signing key, that key may be changed often; from that time on, only the new key will be used for certificate signing purposes. The older, but still valid, certificate will be available to verify old signatures until all of the certificates signed using the associated private key have also expired. If the old private key is used to sign CRLs that contain certificates signed with that key, then the old key must be retained and protected.

A Subscriber certificate may be automatically re-keyed if the public key has not reached the end of its validity period, the associated private key has not been compromised, and the Subscriber name and attributes are unchanged.

4.7.2 Certificate Recovery

Certificate recovery is defined as creating a new certificate with the same Subject name, encryption key, and other information as the old one, but placing a new, extended validity period and a new serial number on the certificate. Generally, certificate recovery is required when a Subscriber no longer has access to their private keys due to loss or corruption of the keys and/or certificates.

Certificate recovery is only applicable to encryption certificates, as identity or verification certificate renewal will always generate new key pairs (i.e., re-key).

4.7.3 Certificate Update

Updating a certificate means creating a new certificate that has the same or a different key and a different serial number, and that differs in one or more other fields, from the old certificate. The old certificate may or may not be revoked, but must not be further re-keyed, renewed, or updated.

If a Subscriber's certificate attributes change, proof of the change must be provided to the RA or LRA, and the Subscriber shall follow the re-key process.

Finally, when any DHS CA updates its private signature key and thus generates a new public key, the CA shall notify all entities that have been issued certificates by the CA (e.g., other CAs, RAs, LRAs, TAs, Subscribers) that it has been changed. For the DHS Root CA, such certificates shall be conveyed to users in a secure fashion to preclude malicious substitution attacks.

4.8 Compromise and Disaster Recovery

In the case of a disaster whereby an operational CA is physically damaged and becomes inoperative but the CA signing key is available, that CA shall be rebuilt, by re-establishing the CA equipment, and operation shall be reestablished as quickly as possible, giving priority to the ability to generate certificate status information.

In case of a CA key compromise, a superior CA shall revoke the compromised CA's certificate and the revocation information shall be published immediately in the most expedient manner. In the event that the revocation information cannot be published immediately, the CA shall securely notify all interested parties (including Subscribers, Subordinate CAs and any cross-certified CAs) at the earliest possible time. Subsequently, the CA installation shall be re-established. The CA shall re-issue all cross-certificates, CA certificates and Subscriber certificates. If the compromised CA is a Root CA, the trusted self-signed certificate shall be removed from each relying party application, and the new one distributed.

In case of a CSA key compromise, the CA that issued the CSA a certificate, shall revoke that CSA's certificate, and the revocation information shall be published immediately. Subsequently, the CSA shall be re-keyed. If the CSA is a trust anchor, the trusted self-signed certificate must be removed from each Relying Party application, and a new one distributed via secure out-of-band mechanisms. The CSA CPS shall describe the approach to reacting to a CSA key compromise.

The DHS PKI OA shall investigate and report to the DHS PKI PA on the cause of any compromise or loss, and what measures have been taken to preclude recurrence.

The DHS PKI directory system shall be deployed so as to provide 24-hour, 365 days per year availability. The DHS PKI OA shall implement features to provide high levels of directory reliability.

In case of a CA key destruction, a superior CA shall revoke the CA's certificate. Subsequently, the CA shall be re-keyed. The CA shall re-issue all cross-certificates, CA certificates and Subscriber certificates. If the CA is a Root CA, the trusted self-signed certificate shall be removed from each relying party application, and a new one distributed. Relying Parties may decide of their own volition whether to continue to use certificates signed with the destroyed private key pending reestablishment of DHS PKI operation with new certificates.

While under recovery from disaster, excluding CA key compromise, the CA(s) shall have the ability to continue operations through offsite backup servers to retain the availability of PKI services.

4.9 CA Termination

In the event of termination of a DHS CA, all certificates issued by the terminated CA shall be revoked and all Subscribers and relying parties promptly notified. In addition, any CA's cross-certified from the terminated CA shall be notified. Reasonable effort shall be made to ensure that discontinuing certification services will cause minimal disruption to its Subscribers and relying parties. Reasonable arrangements to preserve the records of the terminated CA shall be made.

5.0 PHYSICAL, PROCEDURAL AND PERSONNEL SECURITY CONTROLS

5.1 Physical Controls for a DHS CA

Physical security controls shall be implemented that protect the PKI from unauthorized physical access to equipment, facilities, key material, information, and documents, and to safeguard them against espionage, sabotage, damage, tampering, theft, and other covert or overt acts.

Physical security requirements imposed on CAs are likewise imposed on any RAs and LRAs to the extent of their responsibilities and the level of sensitivity of the information they maintain.

5.1.1 Site Location and Construction

The location and construction of the facility housing the CA equipment shall be consistent with facilities used to house high value, sensitive information. The site location and construction, when combined with other physical security protection mechanisms such as guards and intrusion sensors shall provide robust protection against unauthorized access to the CA equipment and records.

5.1.2 Physical Access

The DHS CA and CSA equipment shall always be protected from unauthorized access, and especially while the cryptographic module is installed and activated. Physical access controls shall be implemented to reduce the risk of equipment tampering even when the cryptographic module is not installed and activated. These security mechanisms shall be commensurate with the level of threat in the equipment environment. Access to the CA and CSA equipment and cryptographic tokens shall be limited to specific trusted personnel.

At a minimum, the physical access controls of any DHS CA and CSA shall:

- Ensure no unauthorized access to the hardware is permitted
- Ensure all removable media and paper containing sensitive plain-text information is stored in secure containers

In addition to those requirements, any CA that issues Medium or High assurance certificates shall:

- Be manually or electronically (e.g., via camera) monitored for unauthorized intrusion at all times
- Ensure an access log is maintained and inspected periodically
- Require two-person (or more) integrity physical access control to the CA computer system
- Require two-person (or more) integrity access control to the cryptographic module that holds the CA's private keys

Removable cryptographic modules shall be inactivated before storage. When not in use, removable cryptographic modules, activation information used to access or enable cryptographic modules, and CA equipment shall be placed in secure containers. Activation data shall be either memorized or recorded and stored in a manner commensurate with the security afforded the cryptographic module, and it shall not be stored with the cryptographic module.

A security check of the facility housing the CA and CSA equipment shall occur prior to leaving the facility unattended. At a minimum, the check shall verify the following:

- The equipment is in a state appropriate to the current mode of operation (e.g., that cryptographic modules are in place when “in-use,” and secured when “not in use”)
- Any security containers are properly secured
- Physical security systems (e.g., door locks, vent covers) are functioning properly
- The area is secured against unauthorized access

Additionally, a periodic security check shall be made if the facility is continuously left unattended, to ensure that no attempts to defeat the physical security mechanisms have been made. A person or group of persons shall be made explicitly responsible for making such checks.

A log shall be maintained, identifying the date and time and person performing each check. Each person performing a check shall sign off on the log, asserting that all necessary physical protection mechanisms are in place and activated.

5.1.3 Electrical Power

The facility that houses the CA and CSA equipment shall be supplied with a source of electrical power that is conditioned to protect against brownouts, surges and noise. An uninterruptible source of power will be provided which will supply the required level of power for sufficient duration to ensure that the CA and supporting equipment shall have the capability to automatically lock out input, finish any pending actions, and record the state of the equipment before lack of power or air conditioning causes a shutdown. A backup source of power shall also be supplied to support sustained operations in the event that the primary source of power is inoperable for an extended period of time.

5.1.4 Water Exposures

CA equipment shall be installed such that it is not in danger of exposure to water.

5.1.5 Fire Prevention and Protection

An automatic fire extinguishing system shall be installed in accordance with local policy and code.

5.1.6 Media Storage

Media shall be stored so as to protect it from accidental damage (e.g., water, fire, electromagnetic). Media that contains audit, archive, or backup information shall be duplicated and securely stored in a location separate from the CA(s).

5.1.7 Waste Disposal

Waste containing sensitive information shall be destroyed, such that the information is unrecoverable, prior to disposal. Media used to store sensitive data shall be destroyed, such that the information is unrecoverable, prior to disposal.

5.1.8 Off-Site Backup

Full system backups, sufficient to recover from system failure, shall be made on a periodic schedule as described in the applicable CPS. A current backup shall be created and stored at an offsite location (separate from the PKI equipment) no less than once per week. The backup shall be stored at a facility with physical and procedural controls commensurate to that of the PKI system.

5.2 Procedural Controls

5.2.1 Trusted Roles

All personnel that have access to or control over cryptographic operations that may affect the CA's issuance, use, suspensions, or revocation of certificates, including access to restricted operations of the CA's repository, shall, for purposes of this policy, be considered as serving in a trusted role. A trusted role has special responsibilities, but does not necessarily correspond to special types of Subscribers or certificates.

A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The people selected to fill these roles must be extraordinarily responsible or the integrity of the CA is weakened. The functions performed in these roles form the basis of trust for the entire DHS PKI. Two approaches are taken to increase the likelihood that these roles can be successfully carried out. The first ensures that the person filling the role is trustworthy and properly trained. The second distributes the functions among more than one person, so that any malicious activity would require collusion.

The trusted roles defined in this policy include:

- Administrators—authorized to install, configure, and maintain the CA; establish and maintain user accounts; configure profiles and audit parameters; and generate component keys
- Officers—authorized to request or approve certificates or certificate revocations
- Auditors—authorized to view and maintain audit logs
- Operators—authorized to perform operating system and networking operations

The CPS may define additional trusted roles to provide further role separation, or to include repository responsibilities.

5.2.1.1 Administrators

The Administrator role is responsible for:

- Starting and stopping CA services
- Setting up Security Officers for key recovery
- Backing up and restoring the CA database
- Generation and revocation of certificates for personnel in PKI Trusted Roles
- Posting certificates and CRLs

- Performing the incremental database backups
- Administrative functions such as compromise reporting and maintaining the database
- Hardware cryptographic module programming and management

Administrators do not issue certificates to Subscribers.

5.2.1.2 Officers

The Officer role is responsible for issuing certificates and:

- Verifying a Subscriber's identity, either through personal contact, or via agents or employees, as permitted by this Policy
- Entering user information, and verifying correctness
- Securely communicating requests to and receiving responses from the CA
- Receiving and distributing Subscriber certificate data
- Requesting, approving, and executing the revocation of Subscriber certificates

5.2.1.3 Auditors

PKI Auditors have a view-only role; they can view but not modify audit logs, reports, the Security Policy, and user properties. The PKI Auditors are responsible for maintaining and archiving audit logs and for performing or overseeing internal compliance audits to ensure that CA is operating in accordance with its CPS.

The External Compliance Auditors are different from the PKI Auditor role and may be named in the CPS.

5.2.1.4 Operators

The Operator is responsible for the operation and maintenance of operating system and networking elements of the PKI.

5.2.1.5 CSA Personnel

CSA personnel are the staff that install, configure, administer and operate the CSA.

5.2.2 Separation of Roles

Role separation, when required as set forth in Exhibit 9, may be enforced either by the CA equipment, or procedurally, or by both means.

The separation of roles for the DHS CAs shall be as described in Exhibit 9.

Exhibit 9: Role Separation Requirements

Assurance Level	Role Separation Rules
Test	No stipulation
Rudimentary	No stipulation

Assurance Level	Role Separation Rules
Basic	Individual CA personnel shall be specifically designated to the four roles defined in Section 5.2.1. Individuals may assume more than one role, however, no one individual shall assume both the Administrator and Officer roles. This may be enforced procedurally. No individual shall be assigned more than one identity.
Medium	Individual CA personnel shall be specifically designated to the four roles defined in Section 5.2.1. Individuals may assume more than one role, however, individuals who assume an Officer role may not assume an Administrator or Auditor role. The CA system shall identify and authenticate its users and shall ensure that no user identity can assume both an Administrator and an Officer role, or an Auditor and an Officer role. No individual shall be assigned more than one identity.
High	Individual CA personnel shall be specifically designated to the four roles defined in Section 5.2.1. Individuals may assume only one of the Officer, Administrator, and Auditor roles, but any individual may assume the Operator role. The CA system shall identify and authenticate its users and shall ensure that no user identity can assume both the: <ul style="list-style-type: none"> • Administrator and Officer roles • Administration and Auditor roles • Auditor and Officer roles No individual shall have more than one identity.

5.2.3 Number of Persons Required per Task

No single individual may directly perform operations with the CA private keys. At a minimum, two individuals, preferably using a split knowledge technique, shall be required to perform any CA key issuance, activation, deactivation, recovery, or revocation operation.

5.2.4 Identification and Authentication for Each Role

The identity of all individuals serving in trusted roles must be verified and authenticated before they are issued an account or certificate to carry out their duties. The account or certificate used for a trusted role must only be issued to an individual and must not be shared with other individuals. An individual shall not be allowed to perform actions authorized for a trusted role until they have been identified and authenticated by the system through the use of their account and/or certificate.

5.3 Personnel Controls

5.3.1 Background, Qualifications, Experience, and Security Clearance Requirements

All persons filling trusted roles shall be selected on the basis of loyalty, trustworthiness, and integrity, and shall be a U.S. citizen. The requirements governing the qualifications, selection, and oversight of individuals who operate, manage, oversee and audit the CA and CSA shall be set forth in the respective CPS.

Personnel assigned to operate DHS PKI equipment must:

- Complete an agency background check

- Have no other duties that would interfere with those assigned in support of the PKI
- Have not knowingly been previously relieved of CA, CSA, or Department related security duties for reasons of negligence or non-performance of duties
- Be appointed in writing by the DHS PKI PA

5.3.2 Background Check Procedures

DHS policy shall be followed to perform background checks for personnel identified to serve in trusted roles. Such checks are to be performed solely to determine the suitability of a person to fill a PKI trusted role, and shall not be released except as required by law.

5.3.3 Training Requirements

All personnel performing duties with respect to the operation of the DHS CA and CSA shall receive comprehensive training. Training shall be conducted in the following areas:

- CA/CSA/RA security principles and mechanisms
- All PKI software versions in use on the CA or CSA system
- Disaster Recovery and Business Continuity Procedures
- All other PKI duties they are expected to perform

Documentation shall be maintained identifying all personnel who received training and the level of training completed.

5.3.4 Retraining Frequency and Requirements

Individuals responsible for PKI roles shall be aware of changes in the CA operation. Any significant change to the operations shall have a training (awareness) plan, and the execution of such plan shall be documented. Examples of such changes are CA software or hardware upgrade, changes in automated security systems, and relocation of equipment.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

The DHS PKI PA shall take appropriate administrative and disciplinary actions against personnel who have performed actions involving a DHS CA, CSA, or its repository not authorized in this CP, the applicable CPS, or other procedures published by the OA.

5.3.7 Contracting Personnel Requirements

Contractor personnel employed to perform functions pertaining to the DHS PKI shall meet applicable requirements set forth in this CP and as determined by the DHS PKI PA or OA.

5.3.8 Documentation Supplied to Personnel

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

6.0 TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

This policy does not preclude any end-entity key that has been generated in accordance with the stipulations of this policy and local security requirements, so long as they are generated in cryptographic modules that are Federal Information Processing Standard (FIPS) Publication 140 validated to the level required by this CP as specified in the table in Section 6.2.1.

A key pair is considered to be generated by the PKI entity that first comes into possession of it: a Subscriber, an RA, or a CA. Each entity shall have control over the generation of its own signing key pair. The CA shall not generate Subscriber signing key pairs.

Public-private key pair generation associated with any DHS CA shall be generated in FIPS 140 Security Level 2 (or higher) validated hardware cryptographic modules.

Public-private key pair generation associated with any DHS CSA shall be generated in FIPS 140 Security Level 2 (or higher) validated hardware cryptographic modules.

For all Subscriber certificates, keys shall be generated in a cryptographic module as specified in the table in Section 6.2.1. As stated in Section 6.2.1, for high assurance certificates, subscriber keys shall be generated in FIPS 140 Security Level 2 (or higher) validated hardware cryptographic modules.

All DHS CAs shall document their key generation procedure in their CPSs, and generate auditable evidence that the documented procedures were followed. For all levels of assurance, the documentation of the procedure shall be detailed enough to show that appropriate role separation was used. For High and Medium Assurance the process shall be observed and validated by an independent third party.

6.1.2 Private Key Delivery to Subscriber

A private key shall not appear outside of the module it was generated in, unless it is encrypted. The encrypted private key may be output for local transmission or for storage by a key recovery mechanism.

Each CA private key shall be generated and remain within the cryptographic boundary of the cryptographic hardware module. Therefore, there is no delivery of CA private keys. Accountability for the location and state of the cryptographic module shall be maintained at all times.

Subscriber signature keys shall be generated and remain within the cryptographic boundary of the Subscriber's cryptographic module. Therefore, there is no delivery of Subscriber private signature keys.

In those cases where Subscriber key pairs (other than signature keys) are generated by the CA on behalf of the Subscriber, the private key shall be delivered to the Subscriber in the required hardware or software cryptographic module specified in Section 6.1.1. The delivery mechanism shall provide authentication and confidentiality commensurate with the strength of the cryptography offered by the key.

6.1.3 Public Key Delivery to Certificate Issuer

Subscriber public signature keys shall be delivered to the CA in an authenticated manner defined in the relevant CPS. This shall be done as part of a certificate request. The delivery mechanism shall provide authentication commensurate with the strength of the cryptography offered by the key.

In those cases where key pairs (other than signature keys) are generated by the CA on behalf of the Subscriber, delivery of the public key to the CA is not necessary.

6.1.4 CA Public Key Delivery to Users

Each DHS CA shall post the certificates it issues in the DHS repository. Additionally, the issuing CA's public key and DHS Root CA's public key must be delivered to users, in certificate form, for path validation and to support encrypted communication between the user and the CA. The PKI shall ensure the authenticated and out of band delivery of the DHS Root CA certificate to all DHS PKI Subscribers. The applicable CPS shall detail the specific procedures and mechanisms for the DHS Root CA certificate delivery. The delivery mechanism shall provide authentication commensurate with the strength of the cryptography offered by the DHS Root CA.

The PKI shall ensure the authenticated and out of band delivery of the DHS CSA self-signed certificate(s) to all DHS PKI subscribers. The applicable CPS shall detail the specific procedures and mechanisms for the DHS CSA self-signed certificate delivery. The delivery mechanism shall provide authentication commensurate with the strength of the cryptography offered by the certificates being checked using the CSA.

6.1.5 Key Sizes

All FIPS-approved signature algorithms shall be considered acceptable.

Exhibit 10 identifies the minimum acceptable key lengths for any DHS PKI issued key pairs. Each DHS CA shall detail their current algorithms and key sizes in the applicable CPS.

Exhibit 10: Minimum Acceptable Key Lengths

Assurance Level	Subscribers		CA
	Encryption	Signature	Signature
Test	No Stipulation		
Rudimentary	1024 bit	1024 bit	1024 bit RSA/DSA
Basic	1024 bit	1024 bit	1024 bit RSA/DSA
Medium	1024 bit	1024 bit	2048 bit RSA/DSA
High	1024 bit	1024 bit	2048 bit RSA/DSA

As a minimum, all certificates issued by a DHS CA shall use Secure Hash Algorithm, Version 1 (SHA-1 or better), in accordance with FIPS Pub 186.

Use of Secure Socket Layer (SSL) or another protocol providing similar security to accomplish any of the requirements of this CP shall require at a minimum Triple Data Encryption Standard

(3DES), Advanced Encryption Standard (AES)-128 or other equivalent algorithm for the symmetric key, and at least 1024 bit Rivest-Shamir-Adleman (RSA) encryption algorithm or equivalent for the asymmetric keys.

6.1.6 Public Key Parameters Generation

Public key parameters prescribed in the Digital Signature Standard (DSS) shall be generated in accordance with FIPS 186-2, *Digital Signature Standard (DSS)*.

6.1.7 Parameter Quality Checking

Parameter quality checking (including primarily testing for prime numbers) shall be performed in accordance with FIPS 186-2.

6.1.8 Hardware/Software Key Generation

For Subscribers (except Subscribers for High assurance certificates), software or hardware shall be used to generate pseudo-random numbers, key pairs and symmetric keys. Any pseudo-random numbers used for key generation material shall be generated within a cryptographic module using a FIPS-approved method.

For key generation for CAs and Subscribers for High assurance certificates, the cryptographic modules must be hardware. Refer to Section 6.2.1.

6.1.9 Key Usage

Subscriber keys shall be certified for use in signing, non-repudiation, or encrypting, but may not be certified for multiple use (e.g., signing and encrypting). The use of a specific key is determined by the key usage extension in the X.509 compliant certificate. Certificates to be used for digital signatures shall contain the key usage extension with the *digitalSignature* bit set. Certificates to be used for non-repudiation shall contain the key usage extension with the *nonRepudiation* bit set. Certificates to be used for encryption shall contain the key usage extension with: *keyEncipherment* bit set if the encryption algorithm is a key transfer algorithm such as RSA, or *keyAgreement* bit set if the encryption algorithm is a key agreement algorithm; such as Diffie Hellman or Elliptic Curve Diffie Hellman.

Subscribers shall be configured to use only FIPS-approved encryption algorithms.

6.2 Private Key Protection

6.2.1 Standards for Cryptographic Module

The relevant standard for cryptographic modules is the latest version of the FIPS Pub 140 series, currently FIPS Pub 140-2, *Security Requirements for Cryptographic Modules*.

Exhibit 11 summarizes the minimum requirements for cryptographic modules; higher levels may be used.

Exhibit 11: Minimum Requirements for Cryptographic Modules

Assurance Level	Latest version of FIPS 140 series	Certification Authority	Subscriber	Registration Authority and CSA
Test	No Stipulation			
Rudimentary	N/A	Level 2 (Hardware)	N/A	Level 1 (Hardware or Software)
Basic	Required	Level 2 (Hardware)	Level 1 (Hardware or Software)	Level 1 (Hardware or Software)
Medium	Required	Level 3 (Hardware)	Level 1 (Hardware or Software)	Level 2 (Hardware)
High	Required	Level 3 (Hardware)	Level 2 (Hardware)	Level 2 (Hardware)

All cryptographic modules shall be operated such that the private keys shall never be output in plaintext (unencrypted).

6.2.2 Private Key Multi-Person Control

Multi-person control requires that more than one individual independently authenticate themselves to the system that will perform CA operations. This mechanism prevents any single party (CA or otherwise) from gaining access to the certificate signing key. The private signing key for CAs, including any backup copies, shall only be accessed under two-person control. The CA private signing key may only be backed up under two-person control. The personnel authorized to perform two-person control shall be maintained on a list that shall be made available for inspection during compliance audits.

6.2.3 Private Key Escrow

Under no circumstances shall signature keys used to support non-repudiation or digital signature services be escrowed by a third party.

All private encryption keys shall be escrowed by the CA issuing the Subscriber’s certificate, or by some other trusted escrow system.

6.2.4 Private Key Backup

6.2.4.1 Backup of the CA Private Signature Key

Backup copies of the CA private key shall be made in case the primary module fails. The CA private signature key shall be backed up under the same multi-person control as used to protect the original signature key. A controlled copy or copies of the CA signature key may be stored at various secure locations, as long as all copies of the signature key are controlled, accounted for and protected from unauthorized access to the same degree as the original signature key. Each occurrence of access to a backup copy of the CA private key shall be recorded.

6.2.4.2 Backup of Subscriber Private Signature Keys

Subscriber private signature keys, whose corresponding public key is contained in a certificate asserting the high Assurance policy, may not be backed up or copied.

Subscriber private signature keys whose corresponding public key is contained in a certificate asserting the mediumAssurance, basicAssurance, or rudimentaryAssurance policies may be backed up or copied, but must be held in the Subscriber's control. Backed up keys shall be stored in encrypted form and protected at a level no lower than stipulated for the primary instance of the key.

Backup of a Human Subscriber's private signature key shall not be made for the sole purpose of key recovery.

Component PKI Sponsors (see Section 3.1.10) are authorized to make a single backup copy of the component private keys for continuity of operations purposes to support key recovery in cases where the original key is corrupted.

All key transfers shall be done from and to an approved cryptographic module, and the key shall be encrypted during the transfer. The Human Subscriber, or Sponsor for Components, is responsible for ensuring that all copies of private keys, including those that might be embedded in component backups, are protected, including protecting any system on which the private keys reside.

6.2.5 Private Key Archival

Private keys used to support non-repudiation or digital signature services shall never be escrowed or archived.

The private decryption key shall be encrypted and delivered to the key recovery mechanism associated with the CA. The encryption and delivery mechanism shall provide authentication and confidentiality commensurate with the cryptographic strength of the key being escrowed. The key recovery database may be subject to archival, as described in Section 4.6.

6.2.6 Private Key Entry into Cryptographic Module

Private signature and non-repudiation keys shall be generated by and stored in a cryptographic module. In the event that a private key (other than signature or non-repudiation keys) is to be transported from one cryptographic module to another, the private key must be encrypted during transport. Private keys must never exist in plaintext form outside the cryptographic module boundary.

6.2.7 Method of Activating Private Keys

The Subscriber must be authenticated to the cryptographic module before the activation of any private key(s). Acceptable means of authentication include but are not limited to pass-phrases, PINs or biometrics. Entry of activation data shall be protected from disclosure (i.e., the data should not be displayed while it is entered).

6.2.8 Methods of Deactivating Private Keys

If cryptographic modules are used to store Subscriber private keys, then the cryptographic modules that have been activated shall not be left unattended or otherwise available to unauthorized access. After use, the cryptographic module shall be deactivated, e.g., via a manual logout procedure, or automatically after a period of inactivity as defined in the applicable CPS. Hardware cryptographic modules shall be removed and stored in a secure container when not in use.

Deactivated keys must be cleared from memory before the memory is de-allocated. Any disk space where keys were stored must be overwritten before the space is released to the operating system.

6.2.9 Method of Destroying Subscriber Private Signature Keys

Subscriber private signature keys shall be destroyed when they are no longer needed, or when the certificates to which they correspond expire or are revoked. For software cryptographic modules, this can be overwriting the data. For hardware cryptographic modules, this can be done by executing a “zeroize” command. Physical destruction of hardware is not required.

6.3 Other Aspects of Key-Pair Management

It is technically possible to use the same key-pair for both digital signature and confidentiality. However, this CP discourages that usage for Rudimentary, Basic and Medium. A single dual-use key pair is prohibited for High assurance implementations, where one key-pair shall be used for digital signature/authentication, and a separate key-pair shall be used for confidentiality.

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

CAs use their signing keys for certificate and CRL signing functions. CAs may not issue certificates that extend beyond the expiration dates of their own certificates and public keys. Therefore, their certificate validity periods must be greater than those for Subscribers.

The CAs private signing keys shall be used to sign certificates for not more than one-half of the CAs certificate lifetime.

Exhibit 12 identifies the maximum permissible private key and certificate lifetimes for any DHS PKI key pairs and certificates. Each DHS PKI CA shall specify the specific certificate lifetimes in the applicable CPS.

Exhibit 12: Maximum Permissible Private Key and Certificate Lifetimes

Assurance Level	Subscriber			CA	
	Private Key Lifetime	Certificate Validity Period		Private Key Lifetime	Certificate Validity Period
	Signature/Non-Repudiation	Encryption	Signature / Non-Repudiation	Signature	
Test	No Stipulation				
Rudimentary	5 years	7 years	10 years	10 years	20 years
Basic	5 years	7 years	10 years	10 years	20 years
Medium	2.5 years	3 years	5 years	10 years	20 years
High	2.5 years	3 years	5 years	10 years	20 years

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

The activation data used to unlock CA or Subscriber private keys, in conjunction with any other access control, shall have an appropriate level of strength for the keys or data to be protected. A password, PIN or biometric shall be used as activation data to protect access to private keys, and enforced by the cryptographic module. Activation data shall meet the “strength of authentication mechanism” requirements in FIPS Pub 140-2. Subscribers must have the ability to change their password or PIN.

If the activation data must be transmitted, it shall be via an appropriately protected channel, and distinct in time and place from the associated cryptographic module. If this is not done by hand, the user shall be advised of the shipping date, method of shipping, and expected delivery date of any activation data. As part of the delivery method, users shall sign and return a delivery receipt. In addition, users shall also receive (and acknowledge) a user advisory statement to help them to understand their responsibilities in the use and control of the cryptographic module.

6.4.2 Activation Data Protection

Data used to unlock private keys shall be protected from disclosure by a combination of cryptographic and physical access control mechanisms. Activation data shall either be biometric in nature or memorized, not written down. If written down, it shall be secured at the level of the data that the associated cryptographic module is used to protect, and shall not be stored with the cryptographic module.

The activation data protection mechanism shall include a facility to temporarily lock the account, or terminate the application, after a predetermined number of failed login attempts as defined in the applicable CPS.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

The following computer security functions may be provided by the operating system, or through a combination of operating system, software, and physical safeguards. The PKI computing environment shall include the following functionality:

- Require authenticated logins
- Provide Discretionary Access Control
- Provide a security audit capability
- Restrict access control to CA and CSA services and PKI roles
- Enforce separation of duties for PKI roles
- Require identification and authentication of PKI roles and associated identities
- Residual information protection
- Require use of cryptography for session communication and database security
- Archive CA and CSA history and audit data
- Require self-test security related services
- Require a trusted path for identification and authentication of PKI roles and associated identities
- Require a recovery mechanisms for keys and the CA and CSA system
- Enforce domain integrity boundaries for security critical processes

6.5.2 Computer Security Rating

No Stipulation.

6.6 Lifecycle Technical Controls

Equipment (hardware and software) procured for the DHS PKI shall be purchased in a fashion (such as random selection) to reduce the likelihood that any particular copy was tampered with.

The lifecycle controls for CA and CSA are as follows:

- Hardware and software shall be shipped or delivered via controlled methods that provide a continuous chain of accountability, from origination and throughout its use as CA or CSA equipment. A chain of custody log shall be maintained for all CA and CSA equipment. Tamper-evident packaging shall be used, or equipment shall be hand-carried from a controlled procurement environment to the installation site
- Equipment shall be dedicated to administering a key management infrastructure. It shall not have installed applications or component software, which are not part of the CA or CSA configuration

Reasonable care shall be taken to prevent malicious software from being loaded on RA equipment. Only applications required to perform the organization's mission shall be loaded on the RA computer, and all such software shall be obtained from sources authorized by local policy. Data on RA equipment shall be scanned for malicious code on first use and periodically thereafter.

Equipment updates shall be purchased or developed in the same manner as original equipment, and be installed by trusted and trained personnel in a defined manner.

6.6.1 System Development Controls

The System Development Controls for CA and CSA equipment shall be as follows:

- Use software that has been designed and developed under a formal, documented development methodology
- Hardware and software developed specifically for PKI shall be developed in a controlled environment, and the development process shall be defined and documented

6.6.2 Security Management Controls

The configuration of the PKI system as well as any modifications and upgrades shall be documented and controlled. Methods of detecting unauthorized modifications to the PKI software and configuration shall be in place to ensure the integrity of the security software, firmware, and hardware for correct operation.

A formal configuration management methodology shall be used for installation and ongoing maintenance of DHS CA systems.

DHS CA and CSA software, when first loaded, shall be verified as being that supplied from the vendor, with no modifications, and be the version intended for use.

The integrity of the CA software shall be verified by the DHS PKI OA at least monthly (e.g., in conjunction with ARL publication for the DHS Root CA).

6.7 Network Security Controls

PKI equipment shall be connected to at most one network classification at a time. PKI equipment intended to connect to more than one network classification domain shall have procedures that prevent information from one domain from reaching another (e.g., equipment shutdown, removable hard drives, switching the network connection, etc.).

The PKI equipment shall be protected against network attacks. Use of appropriate boundary controls, such as application level firewalls, shall be employed to protect CA and CSA equipment. Only those network ports associated with protocols and commands required for PKI services shall be allowed. Any network software present on the PKI equipment shall be necessary to the functioning of PKI applications. Root CA equipment shall be configured as stand-alone (off line).

6.8 Cryptographic Module Engineering Controls

Requirements for cryptographic modules are as stated in Section 6.2.

7.0 CERTIFICATE AND CRL PROFILES

7.1 Certificate Profile

7.1.1 Version Numbers

The DHS CAs shall issue X.509 v3 certificates (populate version field with integer “2”).

7.1.2 Certificate Extensions

Certificates issued by the DHS PKI shall comply with *Federal Public Key Infrastructure X.509 Certificate and CRL Extensions Profile* (Federal Public Key Infrastructure [FPKI]-Profile [Prof]). Whenever private extensions are used, they shall be identified in a CPS. Critical private extensions shall be interoperable in their intended community of use.

7.1.3 Algorithm Object Identifiers

Certificates issued under this CP shall use the OIDs listed in Exhibit 13 for signatures.

Exhibit 13: Signature Object Identifiers

Signature Algorithm Identifier	OID
id-dsa-with-sha1	{iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 3}
sha-1WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}
sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
sha384WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 12}
sha512WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 13}
ecdsa-with-SHA1	{iso(1) member-body(2) us(840) ansi-x9-62 (10045) signatures (4) 1 }

Certificates under this CP shall use the OIDs listed in Exhibit 14 for identifying the algorithm for which the subject key was generated.

Exhibit 14: Algorithm Object Identifiers

Algorithm Identifier	OID
id-dsa	{iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 1}
id-ecPublicKey	{iso(1) member-body(2) us(840) ansi-x9-62(10045) public-key-type (2) 1}
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}

7.1.4 Name Forms

Certificate subject name forms shall be X.500 Distinguished Names as described in Section 3.1.1.

7.1.5 Name Constraints

The DHS PKI CAs shall assert name constraints in certificates issued to external CAs appropriate for the CA being certified.

7.1.6 Certificate Policy Object Identifier

Certificates issued under this CP 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 Extension

No stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

Certificates issued under this CP shall not contain policy qualifiers.

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

This policy does not require the certificate policy extension to be critical. Relying parties that do not process this extension do so at their own risk.

7.2 CRL Profile

7.2.1 Version Numbers

All DHS CAs shall issue X.509 Version two (2) CRLs (populate version field with integer “1”).

7.2.2 CRL Entry Extensions

All end-entity PKI software must correctly process all CRL extensions identified in the X.509 version 2 CRL profile. CRL profiles shall comply with FPKI-PROF.

8.0 SPECIFICATION ADMINISTRATION

8.1 Specification Change Procedures

The DHS PKI PA or individual(s) appointed by the DHS PKI PA shall review this CP in its entirety every year to ensure suitability and security. Errors, updates, or suggested changes to this document shall be communicated to the DHS PKI PA for consideration for change. All policy changes under consideration by the DHS PKI PA shall be made available to appropriate parties for review and comment.

The DHS PKI PA shall accept, accept with modifications, or reject the proposed change after completion of the review period.

All updates to this CP shall be made available to all interested parties including CA, Subscribers and Relying Parties.

8.2 Publication and Notification Policies

All Relying Parties, as well as any entity issuing certificates under this policy, shall be notified by the DHS PKI PA prior to making a policy change. This CP and any subsequent changes shall be made publicly available within 1 week of approval.

This CP shall be posted in the repository.

8.3 CPS Approval Procedures

The DHS PKI PA shall be responsible for determining if the CA's CPS complies with this policy.

8.4 Waivers

Waivers to this CP shall not be granted. However, in unforeseen crisis situations, the DHS PKI PA may grant variations in CA practices. Variations in CA practice shall:

- Be deemed acceptable under the current policy
- Require that a change shall be requested to the policy
- Require that a new policy shall be established for the non-compliant practice

Attachment A
Acronyms and Abbreviations

AES	Advanced Encryption Standard
ARL	Authority Revocation List
CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSA	Certificate Status Authority
CSOR	Computer Security Object Registry
DHS	Department of Homeland Security
DN	Distinguished Name
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
FBCA	Federal Bridge Certification Authority
FIPS	Federal Information Processing Standard
FPKI	Federal Public Key Infrastructure
FPKI-Prof	Federal PKI X.509 Certificate and CRL Extensions Profile
FTCA	Federal Tort Claims Act
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
LDAP	Lightweight Directory Access Protocol
LRA	Local Registration Authority
MOA	Memorandum of Agreement (<i>see also</i> Glossary definition)
MOU	Memorandum of Understanding
OA	Operational Authority
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PA	Policy Authority
PCA	Principal Certification Authority
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509 (IETF Working Group)
Pub	Publication
RA	Registration Authority
RFC	Request For Comments
RSA	Rivest-Shamir-Adleman (encryption algorithm)

SBU	sensitive-but-unclassified
SCO	Security Compliance Officer
SCVP	Simple Certificate Validation Protocol
SHA-1	Secure Hash Algorithm, Version 1
S/MIME	Secure Multipurpose Internet Mail Extension
SO	Security Officer
SSL	Secure Sockets Layer
3DES	Triple Data Encryption Standard
TA	Trusted Agent
URL	Uniform Resource Locator
U.S.C.	United States Code
WWW	World Wide Web

Attachment B
Glossary

Access	Ability to make use of any information system (IS) resource.
Access Control	Process of granting access to information system resources only to authorized users, programs, processes, or other systems.
Accreditation	Formal declaration by a Designated Approving Authority that an Information System is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.
Activation Data	Private data, other than keys, that are required to access cryptographic modules (i.e., unlock private keys for signing or decryption events).
Agency	For purposes of this CP only, agency is defined as any instrumentality of the federal government, executive, legislative, or judicial branch.
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.
Archive	Long-term, physically separate storage.
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.
Audit Data	Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event.
Authenticate	To confirm the identity of an entity when that identity is presented.
Authentication	Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual’s identity.
Authority Revocation List (ARL)	A signed, time-stamped list of serial numbers of CA public key certificates, including cross-certificates, that have been revoked.
Backup	Copy of files and programs made to facilitate recovery if necessary.
Binding	Process of associating two related elements of information.
Biometric	A physical or behavioral characteristic of a human being.

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 the certificate's operational period, and (5) is digitally signed by the certification authority issuing it.
Certification Authority (CA)	An authority trusted by one or more users to issue and manage X.509 Public Key Certificates and CRLs.
CA Facility	The collection of equipment, personnel, procedures and structures that are used by a Certification Authority to perform certificate issuance and revocation.
Certification Authority Software	Key Management and cryptographic software used by the CA to generate, revoke, and manage certificates issued to Subscribers.
Certificate Policy (CP)	A Certificate Policy is a specialized form of administrative policy tuned to electronic transactions performed during certificate management. A Certificate Policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery and administration of digital certificates. Indirectly, a certificate policy can also govern the transactions conducted using a communications system protected by a certificate-based security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications.
Certification Practice Statement (CPS)	A statement of the practices that a CA employs in issuing, suspending, revoking and renewing certificates and providing access to them, in accordance with specific requirements (i.e., requirements specified in this CP, or requirements specified in a contract for services).
Certificate Revocation List (CRL)	A list maintained by a Certification Authority of the certificates which it has issued that are revoked prior to their stated expiration date.
Certificate Status Authority (CSA)	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.
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.
Component Private Key	Private key associated with a computer system or software, as opposed to being associated with a human Subscriber.

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.
Computer Security Objects Registry (CSOR)	Computer Security Objects Registry operated by the National Institute of Standards and Technology that assigns the Object Identifiers for its arc.
Confidentiality	Assurance that information is not disclosed to unauthorized entities or processes.
Cross-Certificate	A certificate used to establish a trust relationship between two Certification Authorities.
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.
Data Integrity	Assurance that the data are unchanged from creation to reception.
Digital Signature	The result of a transformation of a message by means of a cryptographic system using keys such that a Relying Party can determine: (1) whether the transformation was created using the private key that corresponds to the public key in the signer's digital certificate; and (2) whether the message has been altered since the transformation was made.
Encryption Certificate	A certificate containing a public key that is used to encrypt electronic messages, files, documents, or data transmissions, or to establish or exchange a session key for these same purposes.
Federal Bridge Certification Authority (FBCA)	The Federal Bridge Certification Authority consists of a collection of Public Key Infrastructure components (Certificate Authorities, Directories, Certificate Policies and Certificate Practice Statements) that are used to provide peer-to-peer interoperability among Entity Principal Certification Authorities.
FBCA Operational Authority	The Federal Bridge Certification Authority Operational Authority is the organization selected by the Federal Public Key Infrastructure Policy Authority to be responsible for operating the Federal Bridge Certification Authority.
Federal Public Key Infrastructure (FPKI) Policy Authority (PA)	The Federal PKI Policy Authority is a federal government body responsible for setting, implementing, and administering policy decisions regarding PKI interoperability that uses the FBCA.
Firewall	Gateway that limits access between networks in accordance with local security policy.

Integrity	Protection against unauthorized modification or destruction of information. A state in which information has remained unaltered from the point it was produced by a source, during transmission, storage, and eventual receipt by the destination.
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.
Key Escrow	A deposit of the private key of a Subscriber and other pertinent information pursuant to an escrow agreement or similar contract binding upon the Subscriber, the terms of which require one or more agents to hold the Subscriber's private key for the benefit of the Subscriber, an employer, or other party, upon provisions set forth in the agreement.
Key Generation Material	Random numbers, pseudo-random numbers, and cryptographic parameters used in generating cryptographic keys.
Key Pair	Two mathematically related keys having the properties that (1) one key can be used to encrypt a message that can only be decrypted using the other key, and (ii) even knowing the public key, it is computationally infeasible to discover the private key.
Local Registration Authority (LRA)	A Registration Authority with responsibility for a local community.
Memorandum of Agreement (MOA)	Agreement between the Federal PKI Policy Authority and an Entity allowing interoperability between the Entity Principal CA and the FBCA. As used in the context of this CP, between an Entity and the Federal PKI Policy Authority allowing interoperation between the FBCA and Entity Principal CA.
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. Technical non-repudiation refers to the assurance a Relying Party has that if a public key is used to validate a digital signature, that signature had to have been made by the corresponding private signature key. Legal non-repudiation refers to how well possession or control of the private signature key can be established.
Object Identifier (OID)	A specialized formatted number that is registered through ISO. For example, CSOR registers OIDs. Yet another example of OIDs are the Certificate Policies OID listed in Section 1.3 of this CP.
Physically Isolated Network	A network that is not connected to entities or systems outside a physically controlled space.

PKI Sponsor	Fills the role of a Subscriber for non-human system components that are named as public key certificate subjects, and is responsible for meeting the obligations of Subscribers as defined throughout this CP.
Policy Authority (PA)	Authority established to oversee the creation and update of Certificate Policies, review Certification Practice Statements, review the results of CA audits for policy compliance, evaluate non-domain policies for acceptance within the domain, and generally oversee and manage the PKI certificate policies.
Principal CA	The Principal CA is a CA designated by an Entity to interoperate with the FBCA. An Entity may designate multiple Principal CAs to interoperate with the FBCA. For the DHS, the DHS Root CA is the Principal CA.
Privacy	Restricting access to Subscriber or Relying Party information in accordance with applicable law and policy.
Private Key	(1) The key of a signature key pair used to create a digital signature. (2) The key of an encryption key pair that is used to decrypt information. In both cases, this key must be kept secret.
Public Key	(1) The key of a signature key pair used to validate a digital signature. (2) The key of an encryption key pair that is used to encrypt information. In both cases, this key is made publicly available normally in the form of a digital certificate.
Public Key Infrastructure (PKI)	A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.
Registration Authority (RA)	An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., a Registration Authority is delegated certain tasks on behalf of an authorized CA).
Re-key (a certificate)	To change the value of a cryptographic key that is being used in a cryptographic system application; this normally entails issuing a new certificate for the new public key.
Relying Party	A person or Entity who uses a certificate (e.g., to verify a digital signature, to establish encrypted communication, to authenticate an entity, etc.)
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 database containing information and data relating to certificates as specified in this CP; may also be referred to as a directory.
Revoke a Certificate	To prematurely end the operational period of a certificate effective at a specific date and time.
Risk	An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.
Root CA	In a hierarchical PKI, the CA whose public key serves as the trusted datum (i.e., the beginning of trust paths) for a security domain.
Secret Key	A “shared secret” used in symmetric cryptography. A single key is shared between two parties: the sender, to encrypt a transmission, and the recipient, to decrypt the transmission, with the shared key being generated or transmitted using other secure means.
Security Compliance Officer	The Security Compliance Officer is responsible for performing ongoing audit oversight of CA operations on behalf of the DHS PKI Policy Authority and DHS PKI Operational Authority, to ensure compliance with this CP, the CA’s CPS and the CA’s operating procedures.
Server	A system entity that provides a service in response to requests from clients.
Signature Certificate	A public key certificate that contains a public key intended for verifying digital signatures.
Subordinate CA	In a hierarchical PKI, a CA whose certificate signature key is certified by another CA, and whose activities are constrained by that other CA. (See superior CA).
Subscriber	A Subscriber is an entity that (1) is the subject named or identified in a certificate issued to that entity, (2) holds a private key that corresponds to the public key listed in the certificate, and (3) does not itself issue certificates to another party. This includes, but is not limited to, an individual or components
Superior CA	In a hierarchical PKI, a CA who has certified the certificate signature key of another CA, and who constrains the activities of that CA. (See subordinate CA).
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.

Token	Hardware or software that contains or can be used to generate cryptographic keys. Examples of hardware tokens include smart cards and memory cards. Software tokens include both software cryptographic modules that store or generate keys and storage devices or messages that contain keys (e.g., PKCS #12 messages).
Trust List	Collection of trusted certificates used by Relying Parties to authenticate other certificates.
Trusted Agent	Entity authorized to act as a representative of an Entity in confirming Subscriber identification during the registration process. Trusted Agents do not have automated interfaces with Certification Authorities.
Two-Person Control	Continuous surveillance and positive control of 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.
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.
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.

Attachment C
References

Request for Comments (RFC) 2527: *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*, March 1999, <http://www.ietf.org/rfc>

X.509 Certificate Policy for the Federal Bridge Certification Authority (FBCA), September 27, 2004, <http://csrc.nist.gov/pki/fbca>

Generic X.509 Certificate Policy Template for the Rudimentary Assurance Level Public Key Infrastructure, Version 1.1, National Institute of Standards and Technology (NIST), June 10, 2002

Records Management Guidance for PKI-Unique Administrative Records, Fifth Draft, December 9, 2002, <http://cio.doe.gov/RBManagement/Records/02.htm>

X.509 Certificate Policy for the United States Department of Defense, Version 5.2, November 13, 2000

PKI Assessment Guidelines, American Bar Association, June 18, 2001

RFC 3280: *Internet X.509 Public Key Infrastructure Certificate and CRL Profile*, April 2002, <http://www.ietf.org/rfc>

Federal PKI X.509 Certificate and CRL Extensions Profile (FPKI-PROF), July 1, 2002, http://csrc.nist.gov/pki/twg/y2002/doc_reg_02.htm

Federal Information Processing Standards (FIPS) Publication (Pub) 140-2: *Security Requirements for Cryptographic Modules*, May 2001, <http://www.itl.nist.gov/fipspubs>

FIPS 186-2: *Digital Signature Standard (DSS)*, January 2000, <http://www.itl.nist.gov/fipspubs>