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

September 28, 2006
Version 3.0

SIGNATURE PAGE

28 Sept 2006

*Department of Homeland Security Public Key Infrastructure
Policy Authority*

Date

CONTENTS

1.0 INTRODUCTION

The Department of Homeland Security (DHS) Public Key Infrastructure (PKI) was implemented to increase the security posture of the organization. The PKI consists of products and services that provide and manage X.509 public key certificates.

This Certificate Policy (CP) defines seven certificate policies for use by the Department of Homeland Security (DHS) Public Key Infrastructure (PKI), i.e., Rudimentary, Internal Basic, Basic, Card Authentication, Medium, Medium Hardware, and High. Each policy establishes a different level of assurance for public key certificates. The level of assurance of a certificate refers to the strength of the binding between the public key and the entity whose subject name is cited in the certificate, the mechanisms used to control the use of the private key, and the security provided by the PKI itself.

The DHS PKI consists of an off-line DHS Root Certification Authority (CA), subordinate DHS CAs that issue certificates at one or more of the assurance levels (Rudimentary, Internal Basic, Basic, Medium, Card Authentication, Medium Hardware, and High), Registration/Local Registration Authorities, Repositories to make information available to Relying Parties, and the Subscribers associated with these CAs.

The DHS Root CA shall act as the Principal CA (PCA) for cross certification with the Federal Bridge CA (FBCA) to enable interoperability with other entity PKIs that have also cross certified with the FBCA. The DHS Root CA may also issue certificates to subordinate DHS CAs, to individuals who operate the DHS Root CA, and cross certificates to External Entity CAs.

Any use of or reference to this DHS CP outside the purview of the DHS PKI Policy Authority (DHS PKI PA) is completely at the using party's risk. CAs not subordinated to the DHS Root CA shall not assert DHS Certificate Policies in any certificates they issue. Subordinate DHS CAs shall only assert those DHS Certificate Policies in the certificates they issue, that are asserted in a certificate issued by the DHS Root CA to the subordinate CA.

When an External Entity CA (a CA that is not part of the DHS PKI) is cross certified with the DHS Root CA, that Entity CA may assert the appropriate DHS Certificate Policies in the *policyMappings* extension of the certificates issued by the External Entity CA for the purpose of establishing an equivalency between a DHS Certificate Policy and an Entity CA Certificate Policy. This use of DHS Certificate Policies shall be limited to that explicitly defined in a memorandum of agreement between the DHS PKI PA and the External Entity CA.

This CP is compliant with the High, Medium Hardware, Medium, Basic, and Rudimentary assurance level policies in the X.509 Certificate Policy for the Federal Bridge Certification Authority. The Card Authentication policy in this CP is compliant with the Common Card Authentication policy in the X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework. The Internal Basic policy is a DHS policy that is defined by this CP and is not related to any external U.S. Federal Certificate Policy.

This DHS CP is consistent with the Internet Engineering Task Force (IETF) *Public Key Infrastructure X.509 (IETF PKIX) Request for Comment (RFC) 3647, Certificate Policy and Certification Practices Statement Framework* [RFC 3647].

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

Note: The term "certificate policy" or "CP" may be used in this document to refer to a single certificate policy document (e.g., this document), even if the document addresses more than one level of assurance policy (e.g., High, Medium, Basic). "Certificate policy" or "CP" may also be used to refer to any one of those levels of assurance certificate policies addressed in the document (e.g., the High assurance level certificate policy).

1.1 Overview

1.1.1 Certificate Policy (CP)

Certificates issued by CAs in the DHS PKI contain a registered certificate policy object identifier (OID), which may be used by a Relying Party to decide whether a certificate is trusted for a particular purpose. The OID corresponds to a specific level of assurance, associated with a specific certificate policy, which shall be available to Relying Parties. Each certificate issued by a DHS CA will assert the specific DHS policy that the certificate is issued under by inserting the corresponding DHS policy OID in the *certificatePolicies* extension on the certificate.

Where the DHS policy under which a certificate is issued meets or exceeds the requirements of other lower level of assurance DHS policies, those lower level of assurance DHS policy OIDs may also be asserted by listing them in the *certificatePolicies* extension on the certificate. The Certification Practices Statement for each DHS CA shall distinguish between each DHS policy under which it can issue a certificate, and the lower level of assurance DHS policy or policies that will also be asserted in the *certificatePolicies* extension on the certificate.

1.1.2 Relationship Between the DHS CP and DHS CPSs

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

1.1.3 Relationship between the FBCA CP and the DHS CP

The FBCA CP defines multiple levels of assurance for certificates and the certificate policies that establish those assurance levels. The Federal PKI Policy Authority (FPKIPA) has mapped the DHS High, Medium and Basic assurance policies to the FBCA High, Medium and Basic assurance policies and determined an equivalency indicated in the Table below.

Equivalence of Certificate Policies	
DHS	**FBCA**
DHS High Assurance	FBCA High Assurance

DHS Medium Assurance	FBCA Medium Assurance
DHS Basic Assurance	FBCA Basic Assurance

This equivalency of policies is asserted in CA certificates issued to the DHS Root CA by the FBCA, and in certificates issued to the FBCA by the DHS Root CA in the *policyMappings* extension. This process is known as cross certification.

Note: Once this CP has been approved, the DHS will apply to the FPKIPA to cross certify at the Medium Hardware level of assurance.

The DHS shall maintain its CP to ensure the continued equivalency of DHS and FBCA policies at each level of assurance at which they are cross certified.

1.1.4 Scope

The DHS PKI exists to facilitate the missions of the DHS and its Components, and to facilitate trusted electronic transactions with other organizations in support of these missions and U.S. Federal Government objectives. This CP defines the certificate policies for the DHS PKI that enables it to meet these objectives. This CP applies to certificates issued to CAs, human subscribers, groups, applications, code signers and devices.

1.1.5 Interoperability with PKIs External to the DHS

The DHS will extend PKI interoperability with non-DHS entities only when it is beneficial to the mission of the Department of Homeland Security and the U.S. Federal Government. Interoperability will be primarily achieved through policy mapping and cross certification with the FBCA. Policy mapping and cross certification with other PKIs may be employed to achieve interoperability that is not available through the FBCA.

1.1.6 Deadline for Compliance With Policy Changes Introduced by this CP

New DHS CAs that initiate operations after this CP is approved, shall be operated in compliance with this CP from their inception.

Existing DHS CAs, operating under the previous approved version of this DHS CP, shall implement the revised practices required to comply with the policy changes implemented by this DHS CP as soon as practical, but no later than August 31, 2007. The DHS PKI Policy Authority may require existing DHS CAs to comply with specific policy changes prior to August 31, 2007.

1.2 Document Identification

There are seven policies specified at seven levels of assurance in this Certificate Policy, which are defined in subsequent sections of this CP. Each level of assurance has an Object Identifier (OID), to be asserted in certificates issued by DHS CAs, as appropriate. The FBCA and External Entity CAs that are cross certified with the DHS Root CA may assert these OIDs in policyMappings extensions of certificates issued to the DHS Root CA, as appropriate. The DHS policy OIDs are registered in the NIST Computer Security Objects Registry as follows:

csor-certpolicy OBJECT IDENTIFIER	::= {2 16 840 1 101 3 2 1 }
dhs-policies OBJECT IDENTIFIER	::= {csor-certpolicy 15}
id-dhs-certpcy-rudimentary	::= dhs-policies 1
id-dhs-certpcy-basic	::= dhs-policies 2
id-dhs-certpcy-medium	::= dhs-policies 3
id-dhs-certpcy-high	::= dhs-policies 4
id-dhs-certpcy-mediumHardware	::= dhs-policies 5
id-dhs-certpcy-cardAuth	::= dhs-policies 6
id-dhs-certpcy-internalBasic	::= dhs-policies 7

The High Assurance policy is reserved for government (federal, state, and local) use.

The requirements associated with the Medium Hardware policy are identical to those defined for the Medium Assurance policy, with the exception of Subscriber cryptographic module requirements (see Section 6.2.1).

The Card Authentication policy is asserted in certificates issued to Personal Identity Verification PIV) Cards, as defined in Federal Information Processing Standard 201 [FIPS 201], supporting card authentication where the private key can be used without Cardholder activation of the card with their PIN. The requirements associated with the Card Authentication policy are the same as those defined for the Medium Hardware policy, with the exception that the private key can be used without activation of the card by the Cardholder. Since the private key can be used without Cardholder activation, no assurance can be associated with this policy.

The Internal Basic policy is a low level of assurance policy for DHS internal use only. Its intended use is for issuing certificates to support the DHS internal networked infrastructure such as for machine-to-machine authentication on internal DHS networks and for encryption of files stored on DHS laptops and mobile devices.

There are seven DHS test policies in this Certificate Policy, which are established to support pilots and testing. DHS test policies have no level of assurance, and are not addressed further in this CP. These test policy OIDs should never be asserted in "real" certificates, and no relying party should ever accept such a certificate to implement security services in a "real" application. The seven DHS test policy OIDs are registered in the NIST Computer Security Objects Registry as follows:

id-dhs-certpcy-testRudimentary	::= dhs-policies 31
id-dhs-certpcy-testBasic	::= dhs-policies 32
id-dhs-certpcy-testMedium	::= dhs-policies 33
id-dhs-certpcy-testHigh	::= dhs-policies 34
id-dhs-certpcy-testMeduimHardware	::= dhs-policies 35
id-dhs-certpcy-testCardAuth	::= dhs-policies 36
id-dhs-certpcy-testInternalBasic	::= dhs-policies 37

1.3 PKI Entities

The following are roles relevant to the administration and operation of the DHS PKI.

1.3.1 PKI Authorities

1.3.1.1 DHS PKI Policy Authority (DHS PKI PA)

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

Robert West
DHS Chief Information Security Officer
Office of Chief Information Officer
Department of Homeland Security

The DHS PKI Policy Authority is responsible for the following:

- All DHS PKI Certificate Policies;
- Approving DHS Certificate Policies;
- Approving the CPSs for each CA that issues certificates under DHS Certificate Policies;
- Ensuring the continued conformance of each DHS CA that issues certificates under this policy with applicable requirements as a condition for allowing continued operation;
- Authorizing the DHS Root CA to issue or revoke certificates to a DHS Subordinate CA;
- Authorizing new DHS CAs to commence operations;
- Directing a DHS CA to cease or suspend operations;
- Authorizing a DHS CA that has ceased or suspended operations to re-start operations;
- Approving all cross certifications by the DHS Root and DHS 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 shall establish the mappings between the DHS assurance policies contained in this CP and the Entity assurance policies contained in the Entity's CP. When the External Entity CA 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;

  Note: The term "MOA," as used in this CP, shall always refer to the Memorandum of Agreement cited in this paragraph.

- Authorizing the DHS Root CA or DHS Subordinate CA to issue or revoke cross certificates to another CA;
- Ensuring continued conformance of all cross-certified External Entity CAs to applicable requirements as set forth in the MOA as a condition for allowing continued cross certification with a DHS Certification Authority;
- Appointing an Alternate DHS PKI PA;

  The Alternate DHS PKI PA is a DHS government employee who performs the DHS PKI PA role, in the event that the DHS PKI PA is unavailable, or unable to perform the duties assigned by this CP.

  Duties assigned to the DHS PKI PA by this CP may be delegated by the DHS PKI PA to the Alternate DHS PKI PA, to perform on an ongoing basis.

  The Alternate DHS PKI PA is appointed by identification in this CP immediately below.

  The Alternate DHS PKI Policy Authority is:

  Don Hagerling
  Director of Security Policy and Security Architecture
  Office of the Chief Information Security Officer
  Department of Homeland Security

- Appointing a DHS PKI Operational Authority (DHS PKI OA);

  The DHS PKI OA is a DHS government employee who performs the functions described in Section 1.3.1.2 of this CP.

  The DHS PKI OA is appointed by identification in this CP immediately below:

  The DHS PKI Operational Authority is:

  William Morgan, Jr.
  Chief Technology Officer
  U.S.VISIT
  Department of Homeland Security

- Appointing an Alternate DHS PKI OA;

The Alternate DHS PKI OA is a DHS government employee who performs the DHS PKI OA role, in the event that the DHS PKI OA is unavailable, or unable to perform the duties assigned by this CP.

The Alternate DHS PKI OA is appointed by identification in this CP immediately below:

The Alternate DHS PKI Operational Authority is:

G. E. Woodford
Acting Director Office of Information Systems Security
Immigration and Customs Enforcement
Department of Homeland Security

- Appointing DHS PKI personnel to PKI Trusted Roles, other than Local Registration Authorities and Trusted Agents;
- Appointing DHS employees to be CA Key Custodians for the DHS CA signing keys; and
- Appointing DHS government employee(s) knowledgeable of PKI, not directly involved in DHS PKI operations, to work with the DHS PKI Policy Compliance Officer to witness DHS CA Key Generation Ceremonies, and to review policy mappings to the DHS CPs of Certificate Practices Statements for DHS Subordinate CAs and External Entity CAs, proposing to cross certify with a DHS CA.

1.3.1.2 DHS PKI Operational Authority (DHS PKI OA)

The DHS PKI Operational Authority (DHS PKI OA) is a DHS government employee, 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 Alternate DHS PKI OA performs the DHS PKI OA role, in the event that the DHS PKI Operational Authority is unavailable, or unable to perform the duties assigned by this CP.

The DHS PKI Operational Authority is responsible for the following:

- Maintaining the CPS for each CA that issues certificates under DHS Certificate Policies;
- Approving the Operating Procedures for each CA that issues certificates under DHS Certificate Policies;
- Providing oversight of DHS PKI services, operations and infrastructure related to certificates issued under this CP to ensure that they are in accordance with the requirements, representations, and warranties of this CP;
- Nominating DHS PKI personnel for appointment to PKI Trusted Roles, other than Local Registration Authorities and Trusted Agents; and
- Appointing DHS PKI personnel as Local Registration Authorities.

Duties assigned to the DHS PKI OA by this CP may be delegated by the DHS PKI OA to the Alternate DHS PKI OA, to perform on an ongoing basis.

For DHS CAs dedicated to issuing certificates for PIV Cards in compliance with FIPS 201, see Section 1.3.2.3 that describes the shift of some responsibilities above associated with Local Registration Authorities to the PIV Card Issuing Organization.

1.3.1.3 DHS PKI Service Manager (PSM)

The DHS PKI Service Manager (PSM) is a DHS PKI Trusted Role. The PSM is a DHS government employee or DHS contractor who is nominated by the DHS PKI OA and appointed by the DHS PKI PA. Both a PSM and an Alternate PSM shall be appointed. The DHS PSM reports to the DHS PKI OA.

The DHS PKI Service Manager is responsible for the following:

- 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 and the relevant CPSs;
- Creating and maintaining the Operating Procedures for each CA that issues certificates under DHS Certificate Policies;
- Recommending DHS PKI personnel for appointment to PKI Trusted Roles, other than Local Registration Authorities and Trusted Agents;
- Managing the operations of the DHS PKI; and
- Performing the DHS Information Systems Security Officer role for the DHS Digital Identity Management Center.

For DHS CAs dedicated to issuing certificates for PIV Cards in compliance with FIPS 201, see Section 1.3.2.3 that describes the shift of some responsibilities above associated with Local Registration Authorities to the PIV Card Issuing Organization.

1.3.1.4 DHS PKI Policy Compliance Officer (PPCO)

The DHS PKI Policy Compliance Officer (PPCO) is a DHS PKI Trusted Role. The PPCO is a DHS government employee or DHS Contractor who is nominated by the DHS PKI OA and appointed by the DHS PKI PA. The DHS PPCO reports to the DHS PKI PA.

The DHS PKI PPCO is responsible for the following, in support of the DHS PKI PA:

- Developing and maintaining DHS Certificate Policies;
- Publishing approved DHS Certificate Policies;
- Developing and maintaining the Certification Practices Statement for the DHS Root CA, and for other CAs, as directed;
- Reviewing and mapping Certificate Practices Statements for DHS Subordinate CAs and External Entity CAs, proposing to cross certify with a DHS CA, to the DHS CPs;
- Coordinating annual and ad hoc compliance audits by the DHS PKI Auditor;
- Performing the Auditor Trusted Role, as defined in this CP (see Section 5.2.1.2);

- Performing ongoing audit oversight of DHS PKI operations to ensure compliance with DHS Certificate Policies and DHS CA Certification Practices Statements, identifying potential and actual problem areas and bringing them to the attention of the DHS PKI PA and DHS PKI OA;
- Reviewing Key Generation Scripts and witnessing key generation ceremonies for DHS CAs; and
- Providing guidance on DHS PKI Certificate Policies to DHS PKI personnel and DHS relying parties.

1.3.1.5 DHS PKI CA Key Custodian (CAKC)

The DHS PKI CA Key Custodian (CAKC) is a DHS PKI Trusted Role. The CAKC is a DHS government employee who is nominated by the DHS PKI OA and appointed by the DHS PKI PA. The DHS PKI CAKC reports to the DHS PKI PA.

The DHS PKI CAKC is responsible for the following, in support of the DHS PKI PA:

- Controlling access to DHS CA keying materials containing DHS CA signing keys, including all backups, from the time the keys are generated, until they are destroyed.

1.3.1.6 DHS Principal Certification Authority (CA)

The DHS PKI is a two-tiered hierarchical PKI that has a single CA at the top of the trust hierarchy, known as the DHS Root CA. All other DHS CAs are subordinate to the DHS Root CA in the hierarchy and are referred to as Subordinate CAs. The DHS Principal CA is the CA within the DHS PKI that has been designated to cross-certify directly with the FBCA. The DHS Root CA is the DHS Principal CA.

The DHS Root CA is an entity that includes operational personnel, and hardware and software systems that will create, sign, issue, manage, and store and distribute public key certificates and Certificate Revocation Lists (CRLs). The DHS Root CA issues certificates to DHS Subordinate CAs, cross-certificates to the FBCA and other External Entity CAs, and end-entity certificates to DHS Root CA administrative staff. The DHS Root CA is responsible for all aspects of the issuance and management of a certificate including:

- Control over the registration process;
- Identification and authentication process;
- Certificate manufacturing process;
- Publication of certificates;
- Revocation of certificates;
- Generation and destruction of the DHS Root CA signing keys;
- Re-key of DHS Root CA signing material; and
- Ensuring that all aspects of DHS Root CA operations and infrastructure related to certificates issued under this CP are performed in accordance with the requirements, representations, and warranties of this CP and the DHS Root CA CPS.

1.3.1.7 DHS Subordinate CAs

DHS Subordinate CAs are entities that include operational personnel, and hardware and software systems that will create, sign, issue, manage, and store and distribute public key certificates and Certificate Revocation Lists (CRLs). DHS Subordinate CAs issue certificates to the Subordinate CA's administrative staff and end entities which may include human subscribers, groups, applications, code signers and devices. DHS Subordinate CAs may also issue cross-certificates to other External Entity CAs when authorized by the DHS PKI PA. Each DHS Subordinate CA is responsible for all aspects of the issuance and management of a certificate including:

- Control over the registration process;
- Identification and authentication process;
- Certificate manufacturing process;
- Publication of certificates;
- Revocation of certificates;
- Generation and destruction of the DHS Subordinate CA's signing keys;
- Re-key of DHS Subordinate CA's signing material; and
- Ensuring that all aspects of DHS Subordinate CA operations and infrastructure related to certificates issued under this CP are performed in accordance with the requirements, representations, and warranties of this CP and the DHS Subordinate CA's CPS.

1.3.2 Registration Authority (RA)

The Registration Authority (RA) is the entity that collects and verifies each Subscriber's identity and information for inclusion in the Subscriber's public key certificate. The RA performs its function in accordance with a CPS approved by the DHS PKI PA. The RA is responsible for:

- The registration process;
- The identification and authentication process,
- The renewal, re-key, modification, revocation and suspension process for Subscriber's certificates, and
- Assisting Subscribers with the key recovery process.

1.3.2.1 Local Registration Authority (LRA)

The RA may delegate RA responsibilities to one or more Local Registration Authorities (LRAs), if allowed by the relevant CPS.

1.3.2.2 Trusted Agent (TA)

The Trusted Agent (TA) is an entity who satisfies all the trustworthiness requirements for an RA or LRA and who performs identity proofing as a proxy for the RA or LRA. TAs perform a subset of the functions performed by an RA or LRA. TAs may provide certificate registration instructions to Subscribers, collect Subscriber information, authenticate and verify the Subscriber's identity, and ensure that the Subscriber signs a Subscriber Agreement. TAs can be used to reduce the demands on an RA or an LRA, or to support 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 be used if allowed by the relevant CPS.

1.3.2.3 Personal Identity Certification Card Issuing Organization (PIVCIO)

The DHS Office of Security is the Personal Identity Certification Card Issuing Organization (PIVCIO). The PIVCIO is the DHS organization responsible for issuing Personal Identity Verification (PIV) Cards that comply with FIPS 201 to DHS employees and contractor employees, and for the life cycle management of the cards and their content.

In the context of this CP, the PIVCIO is responsible for the Local Registration Authority function and services for DHS CAs dedicated to issuing certificates for use on PIV Cards, encompassing the issuance and life cycle management of the certificates. These responsibilities include:

- Managing operations of Local Registration Authority services.
- Nominating and appointing qualified personnel as Local Registration Authorities;
- Identifying, documenting, maintaining and approving the Local Registration Authority practices that will be followed for issuing the Personal Identity Verification (PIV) Cards and associated certificates to ensure compliance with FIPS 201;
- Identifying, documenting, maintaining and approving the Operating Procedures that will be employed by Local Registration Authorities for the issuance and life cycle management of PIV Card certificates in compliance with FIPS 201; and
- Providing oversight of Local Registration Authority services, operations and infrastructure to ensure compliance with FIPS 201 and guidance in NIST SP 800-79.

1.3.3 Certificate Status Server (CSS)

DHS may optionally include an authority that provides status information about certificates on behalf of a CA through online transactions. Such an authority is termed a Certificate Status Server (CSS). Examples of CSSs are as follows:

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

Where the CSS is identified in certificates as an authoritative source for revocation information, the operations of that authority are considered within the scope of this CP. Examples include OCSP servers that are identified in the authority information access (AIA) extension. OCSP servers that are locally trusted, as described in RFC 2560, are not covered by this policy.

DHS shall implement a CSS employing OCSP by 1/1/08 to provide status information about certificates supporting Personal Identity Verification [FIPS 201] issued by DHS CAs.

1.3.4 Subscribers and Sponsors

A Subscriber is the entity 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 entities and non-human entities, such as groups, applications, code signers, content signers and devices, where devices include Web servers, network devices, and other devices.

A human entity referred to as a Sponsor must represent a non-human Subscriber in the registration process and is responsible for meeting the obligations of a Subscriber, as defined throughout this document, on behalf of the non-human Subscriber they represent.

Note: CAs are sometimes technically considered to be "Subscribers" in a PKI. However, the term "Subscriber" as used in this document refers only to those who request certificates for uses other than signing and issuing certificates or certificate status information.

1.3.5 Relying Parties

A Relying Party uses a Subscriber's certificate to verify the integrity of a digitally signed message, to identify the creator of a message, or to establish confidential communications with the Subscriber. The Relying Party is responsible for deciding whether or how to check the validity of the certificate by checking the appropriate certificate status information. 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.

This CP makes no assumptions or limitations regarding the identity of Relying Parties. While Relying Parties are generally Subscribers, Relying Parties are not required to have an established relationship with a DHS CA.

1.3.6 Other Participants

DHS CAs and RAs operating under this CP may require the services of other security, community, and application authorities, such as compliance auditors and attribute authorities. The relevant DHS CPS will identify the parties responsible for providing such services, and the mechanisms used to support these services.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

The sensitivity of the information processed or protected using certificates issued by DHS CAs will vary significantly. Relying Parties must evaluate the 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. This evaluation is done by each Relying Party for its application and is not controlled by this CP.

The DHS PKI is intended to support applications involving unclassified information, which can include sensitive unclassified data protected pursuant to Federal statutes and regulations.

To provide sufficient granularity, this CP specifies security requirements at seven, qualitative levels of assurance: Rudimentary, Internal Basic, Basic, Medium, Card Authentication, Medium Hardware, and High.

The following table provides a brief description of the appropriate uses for certificates at each level of assurance defined in this CP. These descriptions are intended as guidance and are not binding.

Assurance Level	Applicability
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.
Internal Basic	This level provides the level of assurance for issuing certificates to support the DHS internal networked infrastructure such as for machine-to-machine authentication on internal DHS networks and for encryption of files stored on DHS laptops and mobile devices.
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.
Card Authentication	This level provides the level of assurance for use in FIPS 201 Personal Identity Verification (PIV) card certificates where the private key can be used without Cardholder activation of the PIV card. It is used in conjunction with Medium Hardware to provide the set of policies required for PIV card implementation.
Medium Hardware	This level is relevant to environments where 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.
High	This level is reserved for cross-certification with government entities and is appropriate for those environments 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.

Federal Relying Parties should review more detailed guidance governing the use of electronic signatures (which include the use of digital certificates) issued by the Office of Management and Budget implementing the Government Paperwork Elimination Act (Federal Register May 2000: Volume 65, Number 85, Page 25508), as well as more detailed subordinate guidance issued by other agencies pursuant to OMB direction (such as Federal Information Processing Standards, NIST Special Publications and electronic record retention guidance provided by the National Archives and Records Administration).

1.4.2 Prohibited Certificate Uses

No stipulation.

1.5 Policy Administration

1.5.1 Organization Administering the Document

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

1.5.2 Contact Person

Questions regarding this CP shall be directed to the DHS PKI Policy Authority, whose address is:

DHS PKI Policy Authority
Office of the Chief Information Security Officer
Department of Homeland Security
7th and D Street SW
Washington, DC 20528

1.5.3 Person Determining Certification Practices Statement Suitability for the Policy

Every CA in the DHS PKI must have a Certification Practices Statement (CPS). The CPS must conform to the relevant policies in this CP. The DHS PKI Policy Authority is responsible for asserting whether the CPS for a DHS CA conforms to the DHS CP.

For DHS CAs dedicated to issuing certificates for FIPS 201 Personal Identity Verification, those sections of the CPS addressing Local Registration Authority functions shall refer to documents maintained by the PIV Card Issuing Organization that define the practices that will be followed.

In the case of CPSs asserting the DHS Rudimentary, Machine Authentication, Basic, Card Authentication, Medium, Medium Hardware, or High policies, the determination of suitability shall be based on an independent compliance auditor's results and recommendations. See Section 8 for further details. To facilitate initial operations of a DHS CA, an initial determination of suitability may be based on the results and recommendations of a policy mapping performed by the DHS PKI Policy Compliance Officer and reviewed by a DHS employee appointed by the DHS PKI PA, who is knowledgeable of PKI and not directly involved in DHS PKI operations. In such cases, the determination of suitability shall be confirmed by an independent compliance auditor during the first compliance audit performed on the CA.

For CAs asserting the DHS Internal Basic policy, the determination of suitability shall be based on the results and recommendations of a policy mapping performed by the DHS PKI Policy Compliance Officer and reviewed by a DHS employee appointed by the DHS PKI PA, who is knowledgeable of PKI and not directly involved in DHS PKI operations.

1.5.4 CPS Approval Procedures

The DHS PKI Operational Authority shall submit the CPS along with:

- A report addressing the results of the policy mapping review and recommendations, prepared by the DHS PPCO and the DHS employee appointed by the DHS PKI PA; or
- A report on a compliance audit performed by the DHS PKI Auditor.

The DHS PA shall accept or reject the CPS based on the accompanying report. If rejected, the DHS PKI OA shall modify the CPS to resolve the identified discrepancies, obtain a revised review report, and resubmit the CPS to the DHS PKI PA with the revised report.

Approval of the CPS can be revoked by the DHS PKI PA based on the results of a subsequent authorized compliance audit.

A DHS CA’s CPS shall be required to meet all facets of its policy. Waivers, while discouraged, may be granted by the DHS PKI PA in order to meet urgent unforeseen operational requirements. When a waiver is granted the DHS PKI PA shall post the waiver on a website accessible by relying parties and shall either initiate a permanent change to the CP or shall place a specific time limit not to exceed one year on the waiver.

Any waivers granted by the DHS PKI PA are considered changes to the corresponding CP, and may result in revocation of the associated cross-certificate by the FPKI PA.

1.6 Definitions and Acronyms

See Sections 11 and 12.

2.0 PUBLICATION & REPOSITORY RESPONSIBILITIES

2.1 Repositories

The DHS PKI is responsible for operation of repositories to support DHS PKI operations.

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.

2.1.1 DHS PKI Repository Obligations

The DHS may use a variety of mechanisms for posting information into repositories as required by this CP. At a minimum, these mechanisms shall include:

- Posting information to an X.500 Directory Server System that is also accessible through the Lightweight Directory Access Protocol (LDAP);
- Posting all PKI provided information in a timely manner;

- Maintaining security to prevent unauthorized access and tampering; and
- Maintaining the availability of the information as required by the certificate information posting and retrieval stipulations of this CP.

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

2.2 Publication of Certification Information

2.2.1 Publication of Certificates and Certificate Status

DHS CAs shall publish all certificates issued by or to the CA and all CRLs issued by the CA in an appropriate DHS PKI repository.

By August 31, 2007, DHS CAs shall implement mechanisms and procedures designed to ensure certificates and CRLs are available for retrieval 24 hours a day, 7 days a week, with a minimum of 99% availability overall per year and scheduled down-time not to exceed 0.5% annually. If a Certificate Status Server (CSS) has been implemented for the DHS CA, the CSS shall also provide the same availability, i.e., 99% availability overall and limit scheduled down-time to 0.5% annually.

Where repository systems are distributed, the availability figures apply to the system as a whole, rather than each component. Availability targets exclude network outages.

2.2.2 Publication of CA Information

The DHS CP shall be made publicly available to DHS Subscribers and DHS Relying Parties on a DHS web site.

Access to CPSs for DHS CAs shall be granted on a need to know basis, and will not be published in DHS repositories.

2.2.3 Interoperability

The DHS PKI will comply with standards-based schemas for directory objects and attributes for publishing DHS certificates and CRLs.

2.3 Frequency of Publication

This CP and any subsequent changes shall be made publicly available within one week of approval.

2.4 Access Controls on Repositories

The DHS PKI shall protect any repository information not intended for public dissemination or modification.

At a minimum, CA certificates and CRLs issued by DHS CAs and CA certificates issued to DHS CAs shall be made available to Federal Relying Parties. Access to information in DHS CA repositories shall be determined pursuant to the rules and statutes that apply to the DHS. Certificates and certificate status information in DHS CA repositories should be publicly available through the Internet wherever reasonable.

3.0 IDENTIFICATION & AUTHENTICATION

3.1 Naming

3.1.1 Types of Names

For DHS CAs, the following rules apply:

- All CA and RA certificates shall include an X.500 Distinguished Name (DN) in the certificate subject name field;
- All certificates issued to end entities, except those issued at the Rudimentary level of assurance and Card Authentication certificates, shall include an X.500 Distinguished Name (DN) in the certificate subject name field;
- Certificates issued at the Rudimentary level of assurance may include a NULL subject DN if they include at least one alternative name form. This CP does not restrict the types of names that can be used at the Rudimentary level;
- Card Authentication certificates may include a NULL subject DN, but must include a non-NULL Subject Alternate Name that is of the Federal Agency Smart Credential Number (FASC-N) name type [FIPS 201], i.e., the FASC-N of the subject's PIV card; and
- The inclusion of a subject alternate name form is optional for all levels except for Card Authentication, where it is mandatory.

The table below summarizes the naming requirements that apply to each level of assurance.

Assurance Level	Naming Requirement
Rudimentary	Non-Null Subject Name, or Null Subject Name if Subject Alternative Name is populated and marked critical
Internal Basic	Non-Null Subject Name, and optional Subject Alternative Name if marked non-critical
Basic	Non-Null Subject Name, and optional Subject Alternative Name if marked non-critical
Card Authentication	Non-Null Subject Alternate Name that is of the FASC-N name type [FIPS 201], and optional Subject Name
Medium	Non-Null Subject Name, and optional Subject Alternative Name if marked non-critical
Medium Hardware	Non-Null Subject Name, and optional Subject Alternative Name if marked non-critical
High	Non-Null Subject Name, and optional Subject Alternative Name if marked non-critical

3.1.2 Need for Names to Be Meaningful

Names used in the certificates issued by DHS CAs must identify the person or object to which they are assigned.

When DNs are used, the directory information tree must accurately reflect organizational structures.

When DNs are used, the common name must respect name space uniqueness requirements and must not be misleading. This does not preclude the use of pseudonymous certificates as defined in Section 3.1.3.

3.1.3 Anonymity or Pseudonymity of Subscribers

DHS CAs shall not issue anonymous certificates.

DNs in certificates issued by DHS CAs may contain a pseudonym (such as a large number) as long as name space uniqueness requirements are met.

3.1.4 Rules for Interpreting Various Name Forms

Rules for interpreting name forms in certificates issued by DHS CAs shall be in accordance with the CA's certificate profile or a referenced certificate profile, and in accordance with approved standards and guidelines approved by the DHS.

Standards may include:

- X.500 for DN;
- RFC-822 for Internet e-mail address;
- Appropriate Internet RFCs for URL and IP address; and
- A description of naming conventions.

3.1.5 Uniqueness of Names

Name uniqueness must be enforced across the name space domain of the DHS PKI. The DHS PKI PA is responsible for ensuring name uniqueness in certificates issued by DHS CAs. DHS CAs and RAs shall enforce name uniqueness.

Each DHS CA shall include the following information in its CPS:

- What name forms shall be used; and
- How they will allocate names within the Subscriber community to guarantee name uniqueness among current and past Subscribers.

3.1.6 Recognition, Authentication, & Role of Trademarks

The DHS PKI PA shall investigate and correct any name duplication in DHS certificates 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.

Consistent with Federal Policy, the DHS CA's will not knowingly use trademarks in names unless the subject has the rights to use that name.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

In all cases where the party named in a certificate generates its own keys that party shall be required to prove possession of the private key that corresponds to the public key in the certificate request.

Practice Note: For signature keys, this may be done by the entity using its private key to sign a value and providing that value to the DHS CA. The DHS CA shall then validate the signature using the party's public key. The DHS PKI Policy Authority may allow other mechanisms that are at least as secure as those cited here.

In the case where a key is generated by the CA or RA either (1) directly on the party's hardware or software token; or (2) in a key generator that benignly transfers the key to the party's token, then proof of possession is not required.

3.2.2 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 PKI OA shall verify the organization identity information, verify the identity information of the requesting representative of the organization and verify the authority of the requestor to act in the name of the organization.

For organizations internal to DHS, 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.

3.2.3 Authentication of Individual Identity

3.2.3.1 Authentication of Human Subscribers

For Subscribers, each DHS CA, and/or associated RAs shall ensure that the applicant's identity information is verified in accordance with the process established by the applicable CP and CPS. Process information shall depend upon the certificate level of assurance and shall be addressed in the DHS CA's CPS. The documentation and authentication requirements shall vary depending upon the level of assurance.

Effective August 31, 2007 for Medium and High Assurance, identity shall be established no more than 30 days before initial certificate issuance.

The DHS CAs and/or associated RAs shall record the information set forth below for issuance of each certificate:

- The identity of the person performing the identification;
- A signed declaration by that person that he or she verified the identity of the applicant as required using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury) or comparable procedure under local law;
- If in-person identity proofing is done, a unique identifying number(s) from the ID(s) of the applicant, or a facsimile of the ID(s);
- The date of the verification; and
- A declaration of identity signed by the applicant using a handwritten signature and performed in the presence of the person performing the identity authentication, using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury) or comparable procedure under local law.

For All Levels: If an applicant is unable to perform face-to-face registration (e.g., a network device or an application), the applicant may be represented by a trusted person already issued a digital certificate by the DHS CA at the same or higher level of assurance as the certificate being sought. This person is the Sponsor for the applicant. 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.

For the Basic and Medium Assurance Levels: An entity certified by a State or Federal Entity as being authorized to confirm identities may perform in-person authentication on behalf of the RA. The certified entity forwards the information collected from the applicant directly to the RA in a secure manner. Packages secured in a tamper-evident manner by the certified entity satisfy this requirement; other secure methods are also acceptable. Such authentication does not relieve the RA of its responsibility to verify the presented data.

The table below summarizes the identification requirements for each level of assurance.

Assurance Level	Identification Requirements
Rudimentary	No identification requirement; applicant may apply and receive a certificate by providing his or her e-mail address
Internal Basic	Identity may be established by the authorized DHS process for requesting and approving relevant changes to the DHS networked infrastructure, such as the addition of a machine to a DHS network, the encryption of stored files on a DHS laptop or mobile device, etc.
Basic	Identity may be established by in-person proofing before a Registration Authority or Trusted Agent; or remotely verifying information provided by

Assurance Level	**Identification Requirements**
	applicant including ID number and account number through record checks either with the applicable agency or institution or through credit bureaus or similar databases, and confirms that: name, date of birth, address and other personal information in records are consistent with the application and sufficient to identify a unique individual. Address confirmation may be obtained by: a) Issuing credentials in a manner that confirms the address of record supplied by the applicant; or b) Issuing credentials in a manner that confirms the ability of the applicant to receive telephone communications at a number associated with the applicant in records, while recording the applicant's voice.
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 ID., or two Non-Federal Government IDs, one of which shall be a photo ID (e.g., Drivers License).
Card Authentication	Identity shall be established by the card management and issuing system as required by [FIPS 201].
Medium Hardware	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 ID., or two Non-Federal Government IDs, one of which shall be a photo ID (e.g., Drivers License).
High	Identity established by in-person appearance before the Registration Authority or Trusted Agent; information provided shall be verified 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).

3.2.3.2 Authentication of Human Subscribers For Group Certificates

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. The DHS CA and/or associated RAs, LRAs or TAs shall record the information identified in Section 3.2.3.1 for a Sponsor for the group before issuing a group certificate (RAs and LRAs) or before requesting issuance of a group certificate (TAs). The Sponsor shall be a trusted person already issued a digital certificate by the DHS CA at the same or higher level of assurance as the certificate being sought. The Sponsor for a Group shall be the Information Systems Security Officer for the group or equivalent.

In addition to the authentication of the Sponsor, the following procedures shall be performed for members of the group:

- The Sponsor (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 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; and
- 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).

3.2.3.3 Authentication of Devices

Some computing and communications devices (routers, firewalls, servers, etc.) will be named as certificate subjects. In such cases, the device must have a human Sponsor. The Sponsor shall be a trusted person already issued a digital certificate by the DHS CA at the same or higher level of assurance as the certificate being sought. The Sponsor is responsible for providing the following registration information:

- Equipment identification (e.g., serial number) or service name (e.g., DNS name);
- Equipment public keys;
- Equipment authorizations and attributes (if any are to be included in the certificate); and
- Contact information to enable the CA or RA to communicate with the sponsor when required.

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); and

- In person registration by the Sponsor, with the identity of the Sponsor confirmed in accordance with the requirements of Section 3.2.3.1.

3.2.4 Non-verified Subscriber Information

Except for the Rudimentary assurance level, information that is not verified shall not be included in certificates.

3.2.5 Validation of Authority

For cross-certification of a CA with a DHS CA, the DHS PKI OA shall validate the representative's authorization to act in the name of the applicant organization.

For subordination of a DHS CA to the DHS Root CA, the DHS PKI OA shall validate the representative's authorization to act in the name of the applicant.

Before issuing content-signer, code signer or group certificates, the CA shall validate the individual's authority to act in the name of the organization.

3.2.6 Criteria for Interoperation

The FPKIPA shall determine the criteria for cross certification with the FBCA. For cross certification with CAs other than the FBCA, the DHS PKI PA shall determine the criteria for cross certification and ensure that existing cross certification with the FBCA is not impacted.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-key

In the event that a routine re-key of the DHS Root CA is required, a new cross certificate will be requested from the FBCA. The identification and authentication process defined in the FBCA CP and the governing MOA will be followed.

In the event that a routine re-key of an external CA cross certified with a DHS CA is required, a new cross certificate will be issued to the external CA by the issuing DHS CA. Before issuance, the external CA shall identify itself through the use of its current signature key or the initial registration process. If it has been more than three years since the external CA was identified as required in Section 3.2, identity shall be re-established through the initial registration process, or as required by the governing MOA.

Subscribers of DHS CAs shall identify themselves for the purpose of routine re-keying as required in table below.

Assurance Level	Routine Re-key Identity Requirements for Subscriber Signature and Encryption Certificates
Rudimentary	Identity may be established through use of current signature key.
Internal Basic	Identity may be established through use of current signature key.

Assurance Level	Routine Re-key Identity Requirements for Subscriber Signature and Encryption Certificates
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.
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.
Card Authentication	Identity may be established in accordance with the requirements specified in [FIPS 201].
Medium Hardware	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.
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.

3.3.2 Identification and Authentication for Re-key after Revocation

After a certificate issued by a DHS CA has been revoked other than during a renewal or update action, the Subscriber is required to go through the initial registration process described in Section 3.2 to obtain a new certificate.

3.4 Identification and Authentication for Revocation Request

Revocation requests, whether submitted electronically or by other means (e.g., in writing) must be authenticated. Requests to revoke a certificate may be authenticated using that certificate's public key, regardless of whether or not the associated private key has been compromised.

4.0 CERTIFICATE LIFE-CYCLE

DHS CAs implementing this Policy shall not certify other CAs or cross-certify with other CAs 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 Application

This section specifies requirements for initial application for certificate issuance.

4.1.1 Application for Cross Certification With The FBCA

The DHS Root CA shall cross certify with the FBCA at High, Medium Hardware, Medium and Basic assurance levels. When applying to cross certify with the FBCA, the DHS Root CA shall fulfill the application requirements as specified in the U.S. Government Public Key Infrastructure Cross-Certification Criteria and Methodology.

4.1.2 Application for Cross Certification With External Entities Other Than The FBCA

DHS CAs implementing this Policy shall not certify other CAs or cross-certify with other CAs 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.

Requests by an Entity for a non-DHS Certification Authority to cross certify with a DHS Certification Authority shall be submitted to the DHS PKI PA using the contact information provided in Section 1.5. The certificate application shall be submitted to the DHS PKI PA by an authorized representative of the requesting Entity. The Entity applying for cross certification is responsible for providing accurate information in their certificate application. The application shall include:

- A written and signed request to cross certify the non-DHS CA with a DHS CA. The request must include a justification for the cross certification;
- The Certificate Policy (CP) for the non-DHS CA written to the format of the *Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 Certificate Policy and Certification Practices Framework* [RFC 3647]. RFC 2527 format may be accepted at the discretion of the DHS PKI PA;
- A proposed mapping between the policies expressed in the requesting Entity's CP and those in the DHS CP;
- A plan for providing access to each other's CRLs and Certificates; and
- A copy of the most recent Compliance Audit Report for the applicant non-DHS CA.

Upon issuance, each cross certificate issued by the DHS Root CA to an External Entity CA shall be manually checked to ensure each field and extension is properly populated with the correct information before the certificate is delivered to the External Entity.

4.1.3 Application for Subordination to the DHS Root CA

As part of the initial DHS Root and Subordinate CA Key Generation Ceremonies, a certificate was issued to a single DHS medium assurance Subordinate CA. Subsequent DHS CAs added to the DHS PKI must subordinate to the DHS Root CA.

Requests by a DHS Entity to subordinate a DHS Certification Authority to the DHS Root CA shall be submitted to the DHS PKI PA using the contact information provided in Section 1.5. An authorized representative of the DHS Entity shall submit the certificate application to the DHS PKI PA. The requesting DHS Entity is responsible for providing accurate information in their certificate application. The application shall include:

- A formal 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 proposed Certification Practices Statement (CPS) for the Subordinate CA written to the format of the *Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 Certificate Policy and Certification Practices Framework* [RFC 3647]. If Online Certificate Status Processing is to be used, the Certification Practices Statement (CPS) must address the practices followed by the Certificate Status Service (CSS);
- A proposed mapping between the submitted CPS and the DHS CP;
- A detailed description of the proposed registration process for the Subordinate CA;
- Documentation of the engineering design for the Subordinate CA including all of its components, networking and communication protocols, the hardware and software products used, and their configuration;
- The proposed plan for integrating/interfacing the Directory and other key components used by the Subordinate CA with their counterparts used by the existing DHS PKI; and
- The proposed Subordinate CA Key Generation Ceremony (KGC) Script.

Upon issuance, each certificate issued by the DHS Root CA to a Subordinate CA shall be manually checked to ensure each field and extension is properly populated with the correct information.

4.1.4 Application for Subscriber Certificates

The Subscriber shall submit the application, or an authorized third party shall submit the application on behalf of the Subscriber, in accordance with the requirements of the applicable CPS. Entities applying for certificates are responsible for providing accurate information on their certificate applications.

4.2 Certificate Application Processing

Information in certificate applications must be verified as accurate before certificates are issued.

4.2.1 Certificate Application Processing for Cross Certification With The FBCA

Certificate application processing shall be performed as specified in the U.S. Government Public Key Infrastructure Cross-Certification Criteria and Methodology.

4.2.2 Certificate Application Processing for Cross Certification With External Entities Other Than The FBCA

The DHS PKI PA will review the request and determine if sufficient interest exists to proceed. The DHS PKI PA will notify the requesting Entity of their decision to proceed or not. If the DHS PKI PA decides to proceed, it will direct the DHS PKI Policy Compliance Officer, appropriate personnel from the DHS PKI Operational Authority, and one or more DHS employees (knowledgeable of PKI but not involved in DHS PKI operations) to:

- Map the requesting Entity’s CP to the DHS CP for the proposed policy mappings;
- Review the Compliance Audit Report;
- Evaluate the plan for providing access to each other’s CRLs and Certificates; and
- Submit findings and recommendations to the DHS PKI PA.

Note: The DHS PKI PA may direct that the DHS PKI Auditor be involved in the performance of these functions, when appropriate.

If the DHS PKI PA decides to proceed, based on the findings and recommendations, the following steps will be executed:

- The requesting Entity will demonstrate interoperability with the DHS CA via tests performed under the direction of the DHS PKI OA;
- The DHS PKI PA will approve cross certification, and notify the requesting Entity;
- The DHS PKI PA and OA and the requesting Entity's PKI PA and OA will execute a Memorandum of Agreement that sets forth the respective responsibilities and obligations of both parties, and the mappings between their certificate policies; and
- The DHS PKI OA and the requesting External Entity CA PKI OA will cross certify in accordance with the MOA. The DHS CA will perform the identification and authentication of the External Entity CA in accordance with Section 3 of this CP, before issuing the cross certificate.

The DHS Root CA will verify the accuracy of the information in the certificate application and perform the identification and authentication of the External Entity CA in accordance with Section 3 of this CP, before issuing the cross certificate.

4.2.3 Certificate Application Processing for Subordination to the DHS Root CA

The DHS PKI PA will review the request and determine if sufficient interest exists to proceed. The DHS PKI PA will notify the requesting DHS Entity of their decision to proceed or not. If the DHS PKI PA decides to proceed, it will charter a Subordination Project Team made up of: the DHS PKI Policy Compliance Officer; knowledgeable engineering, policy and operations personnel representing both the DHS PKI and the Subordinate CA; plus other personnel, as appropriate.

The Subordination Project Team will be responsible for:

- Designing, engineering, implementing, testing and documenting the integrated DHS PKI-Subordinate CA production system;
- Refining and/or developing practices and operating procedures for the Subordinate CA
- Performing the Key Generation Ceremony for the Subordinate CA; and
- Obtaining Federal Information System Management Act (FISMA) Certification and Accreditation of the production system.

The DHS PKI Policy Compliance Officer and one or more DHS employees (knowledgeable of PKI but not involved in DHS PKI operations) appointed by the DHS PKI PA, will be responsible for:

- Reviewing the detailed description of the registration process for the Subordinate CA, and the Subordinate CA's CPS;
- Mapping the Subordinate CA's CPS to the DHS CP at the proposed policies, documenting findings;

- When appropriate, recommending approval of the CPS by the DHS PKI Policy Authority;
- Reviewing the proposed Key Generation Ceremony Script for compliance with relevant portions of the DHS CP, DHS Root CA CPS and the latest version of the Subordinate CA CPS (proposed or approved) and best practices; and
- Witnessing and reporting on the Key Generation Ceremony.

Note: The DHS PKI PA may direct that the DHS PKI Auditor be involved in the performance of these functions, when appropriate.

The DHS PKI PA shall approve the subordination of the CA in two stages:

- In the first stage, the DHS PKI PA authorizes the Key Generation Ceremony to be performed for the Subordinate CA, and
- In the second and final stage, the DHS PKI PA authorizes the Subordinate CA to commence operations and issue certificates to end entities by approving and signing the Certification Practices Statement for the Subordinate CA.

In the interim period between the two stages, the Subordinate CA may issue certificates required for CA operating staff, and a very limited number of certificates required to complete operational readiness testing. The end entity certificates issued for operational readiness testing shall be used only for testing and shall not be used to implement security services to protect DHS operational systems and data. All end entity certificates issued for operational readiness testing shall be revoked prior to the commencement of operations. During this interim period, the CA shall be operated in full compliance with the relevant policies in the DHS CP.

The DHS Root CA will verify the accuracy of the information in the certificate application and perform the identification and authentication of the Subordinated CA in accordance with Section 3 of this CP, before issuing the certificate during the Key Generation Ceremony.

4.2.4 Certificate Application Processing for Subscriber Certificates

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 accuracy of the information in the certificate application;
- Determine that the Subscriber applicant is authorized to be issued the requested certificate (in accordance with this Policy and the applicable CPS);
- In the case of non-human Subscribers, verify the authorization of the designated Sponsor to represent the Subscriber;
- Authenticate and record the identity of the Subscriber or Sponsor (per Section 3.2); and
- Verify possession by the Subscriber or Sponsor of the private key corresponding to the public key that is the subject of the certificate as specified in Section 3.2 and the applicable CPS.

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

4.2.5 Approval or Rejection of Certificate Applications

The DHS PKI PA may approve or reject any certificate application at its discretion.

The CA or RA shall approve Subscriber certificate applications that have been verified to meet all of the requirements as stated in this CP and in the relevant CPS. The CA or RA shall reject certificate applications that do not meet all of the requirements as stated in this CP and in the relevant CPS.

4.2.6 Time to Process Certificate Applications

No stipulation.

4.3 Issuance

4.3.1 Issuance of Cross Certificates With The FBCA

The DHS PKI OA and the requesting FBCA OA will cross certify in accordance with the governing MOA. The source of the certificate request shall be verified before issuance.

Once cross certification has been approved by the FPKIPA, the DHS Root CA shall:

- Build and sign the cross certificate for the FBCA;
- Verify that all of the fields and extensions for the cross certificate issued by the DHS Root CA have been properly populated;
- Make the cross certificate available to the FBCA, and post it to the DHS repository and system;
- Verify that all of the fields and extensions for the cross certificate issued to the DHS Root CA by the FBCA have been properly populated; and
- Post the cross certificate issued to the DHS Root CA by the FBCA to the DHS repository system.

The process for notifying the FBCA of certificate issuance is defined in *U.S. Government Public Key Infrastructure Cross-Certification Criteria and Methodology*, and the governing MOA.

4.3.2 Issuance of Cross Certificates With External Entities Other Than The FBCA

The DHS PKI OA and the requesting Entity PKI OA will cross certify in accordance with the governing MOA. The source of the certificate request shall be verified before issuance.

Once cross certification has been approved by the DHS PKI PA, the DHS Root CA shall:

- Build and sign the cross certificate for the External Entity CA;
- Verify that all of the fields and extensions for the cross certificate issued by the DHS Root CA have been properly populated;
- Make the cross certificate available to the External Entity CA, and post it to the DHS repository system;
- Verify that all of the fields and extensions for the cross certificate issued to the DHS Root CA by the External Entity CA have been properly populated; and
- Post the cross certificate issued to the DHS Root CA by the External Entity CA to the DHS repository system.

The process for notifying the External Entity CA of certificate issuance is defined in the governing MOA.

4.3.3 Issuance of Certificates to Subordinate CAs

The source of the certificate request shall be verified before issuance.

Once the performance of the Key Generation Ceremony has been authorized by the DHS PKI PA, the ceremony will be performed and the DHS Root CA shall:

- Build and sign the Subordinate CA certificate;
- Verify that all of the certificate fields and extension have been properly populated; and
- Make the certificate available to the Subordinate CA, and post it to the DHS repository system.

The DHS PKI Service Manager shall notify the DHS PKI OA of certificate issuance in writing with a signed receipt of notification provided by the DHS PKI OA. Digitally signed emails for notification and receipt may be used.

See Section 4.2.3 for restrictions on the operation of the Subordinate CA certificate until the DHS PKI PA approves and signs the Subordinate CA's CPS.

4.3.4 Issuance of Certificates to Subscribers

The source of the certificate request shall be verified before issuance.

Once the certificate application has been processed and all certificate requirements have been met, the DHS CA shall:

- Build and sign a certificate (or sign the certificate that is built by a Registrar or Subscriber);
- Verify that all of the certificate fields and extension have been properly populated (This may be done through software that scans the fields and extensions looking for any evidence that a certificate was improperly manufactured); and
- Make the certificate available to the Subscriber, and post it to the DHS repository system.

The CPS for a DHS CA shall identify the process for Subscriber notification. Where notification is not an integral component of the issuance process, CAs should proactively notify Subscribers that certificates have been generated.

4.4 Acceptance

4.4.1 Acceptance of Cross Certificates With The FBCA

For the DHS Root CA, failure of the FBCA to object to the certificate or its contents constitutes acceptance of the certificate.

Cross certificates will be posted to the DHS repository system.

The FBCA shall notify the DHS PKI PA of new certificate issuance upon issuance.

The DHS PKI PA shall notify the FPKI PA of new inter-organizational CA cross-certificates upon issuance.

4.4.2 Acceptance of Cross Certificates With External Entities Other Than The FBCA

For the DHS CA, failure to object to the certificate or its contents constitutes acceptance of the certificate.

Cross certificates will be posted to the DHS repository system.

Cross certified External Entity CAs, shall notify the DHS PKI PA of new CA cross-certificates upon issuance.

The DHS PKI PA shall notify the External Entity CA Policy Authority of new CA cross-certificates issued by the DHS CA upon issuance.

Practice Note: The process for notifying the DHS PKI PA and External Entity CA Policy Authority shall be included in the MOA.

4.4.3 Acceptance of Certificates Issued to Subordinate CAs

For the DHS Root CA, failure to object to the certificate or its contents constitutes acceptance of the certificate.

Certificates will be posted to the DHS repository system.

4.4.4 Acceptance of Certificates Issued to Subscribers

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, Medium Hardware, and Medium Assurance level certificates, require the Subscriber to sign documentation indicating acceptance of their responsibilities (as defined in Section 9.6.3); and
- For any certificates issued at other assurance levels, require the Subscriber to acknowledge acceptance of their responsibilities (as defined in Section 9.6.3) - 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.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

The intended scope of usage for a private key is specified in the associated certificate.

For High, Medium Hardware, Medium, Basic Assurance and Internal Basic Subscribers shall protect their private keys from access by other parties. For Rudimentary assurance and Card Authentication, no stipulation.

4.5.2 Relying Party Public Key and Certificate Usage

Certificates issued by DHS CAs specify restrictions on use through critical certificate extensions, including the basic constraints and key usage extensions. DHS CAs issue CRLs specifying the current status of all unexpired DHS CA certificates. It is recommended that relying parties process and comply with this information whenever using certificates issued by DHS CAs in a transaction.

4.6 Certificate Renewal

Certificate renewal consists of issuing a new certificate with a new validity period and serial number while retaining all other information in the original certificate including the public key. Frequent renewal of certificates may assist in reducing the size of CRLs.

4.6.1 Circumstance for Certificate Renewal

The CPS for each DHS CA shall specify whether certificate renewal is supported.

Support for renewal of cross certificates issued by DHS CAs shall be specified in the governing CPS and MOA between the cross certified parties. For cross certificates, the validity period associated with the new cross certificate must not extend beyond the period of the governing MOA.

DHS Root CA certificates issued to DHS Subordinate CAs shall not be renewed.

Subscriber certificates may be renewed when the issuing CA re-keys.

If certificate renewal is supported by a DHS CA, a certificate may be renewed 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. In addition, the validity period of the certificate must meet the requirements specified in Section 6.3.2.

When a Subscriber certificate is renewed, it is not mandatory that the old certificate be revoked, but if it is not revoked, it must not be further re-keyed, renewed, or updated.

4.6.2 Who Can Request Renewal

Requests for renewal of cross certificates shall be made as specified in the governing CPS and MOA between the cross certified parties.

For DHS CAs that support certificate renewal requests for Subscribers, the renewal requests shall only be accepted from the Subscriber who is the subject of the certificate, the authorized Sponsor for the Subscriber, RAs or LRAs.

A DHS CA may perform renewal of its Subscriber certificates without a corresponding request, such as when the CA re-keys.

4.6.3 Processing Certificate Renewal Requests

For DHS CAs that support certificate renewal, the governing CPS shall specify how certificate renewal requests shall be processed.

4.6.4 Notification of New Certificate Issuance to Subscriber

For DHS CAs that support certificate renewal, the governing CPS shall specify how the subjects of the renewed certificates will be notified.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

For DHS CAs that support certificate renewal, the governing CPS shall specify conduct constituting acceptance of a renewal certificate.

4.6.6 Publication of the Renewal Certificate by the CA

All certificates issued by DHS CAs shall be published in the DHS PKI repository system.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

The DHS PKI OA shall notify the DHS PKI PA when a renewal of a cross certificate issued to the FBCA or another External Entity CA occurs. The DHS PKI PA shall determine what external notifications are required based on the applicable MOA.

4.7 Certificate Re-Key

The CPS for each DHS CA shall specify whether certificate re-key is supported.

Re-keying a certificate consists of creating new certificates with a different public key (and serial number) while retaining the remaining contents of the old certificate that describe the subject. The new certificate may be assigned a different validity period, key identifiers, specify a different CRL distribution point, and/or be signed with a different key.

Subscribers of DHS CAs shall identify themselves for the purpose of re-keying as required in Section 3.3.1.

4.7.1 Circumstance for Certificate Re-key

The longer and more often a key is used, the more susceptible it is to loss or discovery. Therefore, it is important that a Subscriber or CA periodically obtain new keys. Sections 5.6 and 6.3.2 establish usage periods for private keys for both DHS CAs and Subscribers.

Certificates may be re-keyed when they can no longer be renewed as described in Section 4.6.

Certificates may be re-keyed when the associated private key is suspected or known to have been compromised.

The DHS Root CA will support the re-keying of DHS Subordinate CAs by issuing a new certificate to the Subordinate CA for the new key pair.

The DHS Root CA will issue a new cross-certificate to the FBCA when the FBCA has generated a new key pair and a valid and unexpired MOA exists between the DHS PKI PA and the FPKIPA. The validity period of the new certificate must not extend beyond the period of the MOA.

When specified in the governing CPS, a DHS CA, which has cross certified with an External Entity CA, may issue a new cross-certificate to External Entity CA when the External Entity CA has generated a new key pair and a valid and unexpired MOA exists between the DHS PKI PA and the External Entity Policy Authority. The validity period of the new certificate must not extend beyond the period of the MOA.

If supported by the issuing DHS CA, Subscriber certificates may be re-keyed. The circumstances governing re-key shall be described in the governing CPS.

4.7.2 Who Can Request Certification of a New Public Key

Requests to re-key the DHS Root CA shall be submitted to the DHS PKI PA by the DHS PKI OA. The DHS PKI PA may direct the DHS PKI OA to re-key the DHS Root CA without a request.

Requests for the DHS Root CA to issue a new cross certificate to the FBCA, after a FBCA re-key, shall be submitted by the FPKIPA or FPKIOA to the DHS PKI PA, or in accordance with the governing MOA.

Requests by an External Entity CA currently cross certified with a DHS CA, for the DHS CA to issue a new cross certificate to the to the External Entity CA after re-key, shall be submitted to the DHS PKI PA by the PKI PA for the External Entity CA, or in accordance with the governing MOA.

Requests for the DHS Root CA to issue a new certificate to a DHS Subordinate CA for a new key pair (re-key) shall be submitted to the DHS PKI PA from the DHS PKI OA.

For DHS CAs that support re-key of Subscriber certificates, re-key requests shall only be accepted from the Subscriber who is the subject of the certificate, the authorized Sponsor for the Subscriber, RAs or LRAs.

Additionally, CAs and RAs may initiate re-key of a Subscriber’s certificates without a corresponding request.

4.7.3 Processing Certificate Re-keying Requests

For DHS CAs that support certificate re-key, the governing CPS shall specify how certificate re-key requests shall be processed.

4.7.4 Notification of New Certificate Issuance to Subscriber

For DHS CAs that support certificate re-key, the governing CPS shall specify how the subjects of the re-keyed certificates will be notified.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

For DHS CAs that support certificate re-key, the governing CPS shall specify conduct constituting acceptance of a re-keyed certificate.

4.7.6 Publication of the Re-keyed Certificate by the CA

All certificates issued by DHS CAs shall be published in the DHS PKI repository system.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

The DHS PKI OA shall notify the DHS PKI PA when a re-key of any certificate issued to an external PKI entity occurs. The DHS PKI PA shall determine what external notifications are required based on the applicable MOA.

4.8 Modification

Certificate modification consists of creating new certificates with subject information (e.g., a name or email address) that differs from the old certificate. The new certificate may have the same or different subject public key. After certificate modification, the old certificate may or may not be revoked, but must not be further re-keyed, renewed, or modified.

4.8.1 Circumstance for Certificate Modification

The CPS for each DHS CA shall specify the circumstances for key modification.

Modifications to cross certificates issued by DHS CAs shall be limited to changes in the cross certified CA’s distinguished name.

A DHS CA may perform certificate modification for a Subscriber whose characteristics have changed (e.g., name change due to marriage). The new certificate may have the same or different subject public key.

After certificate modification, the old certificate may or may not be revoked, but must not be further re-keyed, renewed, or modified.

4.8.2 Who Can Request Certificate Modification

Requests to modify the DHS Root CA certificate shall be submitted to the DHS PKI PA by the DHS PKI OA. The DHS PKI PA may direct the DHS PKI OA to modify the DHS Root CA without a request.

Requests for the DHS Root CA to modify a cross certificate to the FBCA, shall be submitted by the FPKIPA or FPKIOA to the DHS PKI PA, or in accordance with the governing MOA.

Requests by an External Entity CA currently cross certified with a DHS CA, for the DHS CA to modify a cross certificate to the to the External Entity CA, shall be submitted to the DHS PKI PA by the PKI PA for the External Entity CA, or in accordance with the governing MOA.

Requests for the DHS Root CA to modify a certificate issued to a DHS Subordinate CA shall be submitted to the DHS PKI PA by the DHS PKI OA.

For DHS CAs that support modification of Subscriber certificates, modification requests shall only be accepted from the Subscriber who is the subject of the certificate, the authorized Sponsor for the Subscriber, RAs or LRAs.

The CPS for each DHS CA shall specify who can request certificate modification.

4.8.3 Processing Certificate Modification Requests

For DHS CAs that support certificate modification, the governing CPS shall specify how certificate re-key requests shall be processed.

For all DHS CAs, proof of all subject information changes must be provided to the RA, LRA or Trusted Agent and verified before the modified certificate is issued.

4.8.4 Notification of New Certificate Issuance to Subscriber

For DHS CAs that support certificate modification, the governing CPS shall specify how the subjects of the re-keyed certificates will be notified.

4.8.5 Conduct Constituting Acceptance of a Modified Certificate

For DHS CAs that support certificate modification, the governing CPS shall specify conduct constituting acceptance of a modified certificate.

4.8.6 Publication of the Modified Certificate by the CA

All certificates issued by DHS CAs shall be published in the DHS PKI repository system.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

The DHS PKI OA shall notify the DHS PKI PA when the modification of any certificate issued to an external PKI entity occurs. The DHS PKI PA shall determine what external notifications are required based on the applicable MOA.

4.9 Certificate Revocation & Suspension

Certificate suspension is not allowed by this policy.

Revocation requests must be authenticated. Requests to revoke a certificate may be authenticated using that certificate's associated private key, regardless of whether or not the private key has been compromised.

For High, Medium Hardware, Card Authentication, Medium, Basic, and Internal Basic Assurance, all CAs shall publish CRLs.

4.9.1 Circumstance for Revocation

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:

- The identifying information in the certificate becomes invalid;
- When it is determined that cross certification with a CA is no longer in the best interests of the DHS;
- A cross certified CA can be shown to have violated, or is suspected of violating the requirements set forth by this CP or the governing MOA with the DHS;
- A CA subordinated to the DHS Root CA can be shown to have violated, or is suspected of violating the requirements set forth by this CP or the applicable CPS;
- A Subscriber can be shown to have violated, or are suspected of violating the requirements set forth in the Subscriber Agreement;
- A cross certified 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 private keys of a CA subordinated to the DHS Root CA 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;
- A Subscriber'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 authorized representative of a cross certified CA, or other authorized party as defined in the applicable MOA, asks for its certificate to be revoked;
- The authorized representative of a CA subordinated to the DHS Root CA, or other authorized party as defined in the applicable CPS, asks for its certificate to be revoked;
- The Subscriber, or other authorized party as defined in the applicable CPS, asks for their 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 the DHS; and
- 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 CRL. Revoked certificates shall be included on all new publications of the CRL until the certificates expire.

A DHS CA's CPS may specify additional reasons for revocation.

4.9.2 Who Can Request Revocation

A cross certified issued to a CA may be revoked upon direction of the DHS PKI PA or upon an authenticated request by an authorized representative of a cross certified CA as defined in the applicable MOA.

A certificate issued to subordinate CAs may be revoked upon direction of the DHS PKI PA or upon an authenticated request by an authorized representative of the subordinate CA as defined in the applicable CPS

A DHS 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 governing CPS.

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

4.9.3 Procedure for Revocation Request

DHS CAs that implement certificate revocation shall revoke certificates upon receipt of sufficient evidence of compromise or loss of the subscriber's corresponding private key.

Revocation requests must be authenticated. Requests to revoke a certificate may be authenticated using that certificate's associated private key, regardless of whether or not the private key has been compromised.

Upon receipt of a revocation request involving a cross certificate issued to a cross certified CA, the DHS PKI OA shall authenticate the request and apprise the DHS PKI PA. The DHS PKI PA may, at its discretion, take whatever measures it deems appropriate to verify the need for revocation. If the revocation request appears to be valid, the DHS PKI PA shall direct the DHS PKI OA to revoke the certificate. The DHS PKI OA shall give prompt oral or electronic notification to officials authorized to represent the FBCA and other External Entity CAs cross certified with a DHS CA.

Upon receipt of a revocation request involving a certificate issued to a subordinate CA by the DHS Root CA, the DHS PKI OA shall authenticate the request and apprise the DHS PKI PA. The DHS PKI PA may, at its discretion, take whatever measures it deems appropriate to verify the need for revocation. If the revocation request appears to be valid, the DHS PKI PA shall direct the DHS PKI OA to revoke the certificate.

A Subscriber or other authorized individual (see Section 4.9.2) may request revocation of a certificate electronically or in writing. The request to revoke a certificate shall identify the certificate to be revoked, explain the reason for revocation, and allow the request to be authenticated (e.g., digitally or manually signed).

Where Subscribers use hardware tokens, revocation is optional if all the following conditions are met:

- The revocation request was not for key compromise;
- The hardware token does not permit the user to export the signature private key;
- The Subscriber surrendered the token to the PKI;

- The token was zeroized or destroyed promptly upon surrender; and
- The token has been protected from malicious use between surrender and zeroization or destruction.

In all other cases, revocation of the certificates is mandatory. Even where all the above conditions have been met, revocation of the associated certificates is recommended.

4.9.4 Revocation Request Grace Period

The revocation request grace period is the time available to the Subscriber within which the Subscriber must make a revocation request after reasons for revocation have been identified.

In the case of key compromise, cross certified and subordinate CAs are required to request revocation within 1 hour. For all other reasons, they are required to request revocation within 24 hours.

In the case of key compromise and other reasons, Subscribers to DHS CAs are required to request revocation within the time limits specified in the following table.

Assurance Level	**Revocation Request Grace Period**	
	For Key Compromise	**For Other Reasons**
Rudimentary	As Specified in CPS	As Specified in CPS
Internal Basic	As Specified in CPS	As Specified in CPS
Basic	12 hours	24 hours
Medium	2 hours	24 hours
Card Authentication	As Specified in CPS	As Specified in CPS
Medium Hardware	2 hours	24 hours
High	1 hour	24 hours

4.9.5 Time Within Which CA Must Process the Revocation Request

Revocation requests from cross certified and subordinate CAs must be processed within 6 hours of receipt of the request.

Revocation requests from Subscribers to DHS CAs must be processed within the time limits set forth in the following table.

Assurance Level	Processing Time for Revocation Requests
Rudimentary	As Specified in CPS
Internal Basic	As Specified in CPS
Basic	Within 24 hours of receipt of request
Medium	Within 18 hours of receipt of request
Card Authentication	Within 18 hours of receipt of request
Medium Hardware	Within 18 hours of receipt of request
High	Within 6 hours of receipt of request

4.9.6 Revocation Checking Requirements for Relying Parties

Use of revoked certificates could have damaging or catastrophic consequences. The matter of how often new revocation data should be obtained is a determination to be made by the Relying Party, considering the risk, responsibility, and consequences for using a certificate whose revocation status cannot be guaranteed.

4.9.7 CRL Issuance Frequency

For this CP, CRL issuance encompasses both CRL generation and publication.

For the DHS CAs issuing cross certificates to External Entity CAs, the interval between CRLs shall not exceed 24 hours. In the case of revocation of a certificate, an emergency CRL shall be issued within six hours.

For Other DHS CAs, see the table below for issuing frequency of routine and emergency CRLs. For Basic, Medium, Card Authentication, Medium Hardware, and High, Emergency CRLs shall be issued whenever a CA certificate is revoked, or any certificate is revoked because of key compromise. CRLs may be issued more frequently than specified below.

Assurance Level	Maximum Interval for Routine CRL Issuance	Maximum Interval for Emergency CRL Issuance
Rudimentary	As Specified in CPS	As Specified in CPS
Internal Basic	As Specified in CPS	As Specified in CPS
Basic	24 hours	24 hours after notification
Card Authentication	24 hours	18 hours after notification

Assurance Level	Maximum Interval for Routine CRL Issuance	Maximum Interval for Emergency CRL Issuance
Medium	24 hours	18 hours after notification
Medium Hardware	24 hours	18 hours after notification
High	24 hours	6 hours after notification

For the DHS Root CA that only issues CA certificates and is operated in an off-line manner, routine CRLs may be issued less frequently than specified above. However, the interval between routine CRL issuance shall not exceed 31 days. The DHS Root CA must meet the requirements specified above for issuing Emergency CRLs. The DHS PKI OA will also be required to notify the FPKI Operational Authority upon Emergency CRL issuance. This requirement will be included in the MOA between the FPKIPA and the DHS.

4.9.8 Maximum Latency of CRLs

No stipulation. (See Section 4.9.7).

4.9.9 On-line Revocation/Status Checking Availability

If on-line revocation/status checking is supported by a DHS CA, the latency of certificate status information distributed on-line by Entity CAs or their delegated status responders must meet or exceed the requirements for CRL issuance stated in Section 4.9.7.

4.9.10 On-line Revocation Checking Requirements

No stipulation.

4.9.11 Other Forms of Revocation Advertisements Available

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

4.9.12 Special Requirements Related To Key Compromise

In the event of the compromise or loss of a private key belonging to an External Entity CA that is cross certified with a DHS CA, a CRL shall be published at the earliest feasible time by the External Entity, as specified in the MOA.

4.9.13 Circumstances for Suspension

Suspension shall not be used by DHS CAs.

4.9.14 Who Can Request Suspension

Not applicable.

4.9.15 Procedure for Suspension Request

Not applicable.

4.9.16 Limits on Suspension Period

Not applicable.

4.10 Certificate Status Services

No stipulation.

4.10.1 Operational Characteristics

No stipulation.

4.10.2 Service Availability

No stipulation.

4.10.3 Optional Features

No stipulation.

4.11 End Of Subscription

No stipulation.

4.12 Key Escrow & Recovery

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. Escrowed keys shall be protected at no less than the level of security in which they are generated, delivered, and protected by the Subscriber.

4.12.1 Key Escrow and Recovery Policy and Practices

For DHS CAs that support key escrow and recovery, the practices shall be described in their CPSs.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

For DHS CAs that support session key encapsulation and recovery, the practices shall be described in their CPSs.

5.0 FACILITY MANAGEMENT & OPERATIONS CONTROLS

5.1 Physical Controls

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, LRAs and TAs to the extent of their responsibilities and the level of sensitivity of the information they maintain.

5.1.1 Site Location & 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

5.1.2.1 Physical Access for CA Equipment

The DHS CA and CSS 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 CSS equipment and cryptographic tokens shall be limited to specific trusted personnel.

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

- Ensure no unauthorized access to the hardware is permitted; and
- 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, Card Authentication, Medium Hardware 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; and
- 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 CSS equipment (operating at the Basic Assurance level or higher) shall occur if the facility is to be left 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; and
- 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. When a group of persons is responsible, a log identifying the person performing a check at each instance shall be maintained. If the facility is not continuously attended, the last person to depart shall initial a sign-out sheet that indicates the date and time, and asserts that all necessary physical protection mechanisms are in place and activated.

5.1.2.2 Physical Access for RA Equipment

RA equipment shall be protected from unauthorized access while the cryptographic module is installed and activated. The RA shall implement physical access controls 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 RA equipment environment.

5.1.2.3 Physical Access for CSS Equipment

Physical access control requirements for CSS equipment (if implemented), shall meet the CA physical access requirements specified in 5.1.2.1.

5.1.3 Power and Air Conditioning

The facility that houses the CA and CSS 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.

In addition, DHS directories containing certificates and CRLs issued by DHS CAs shall be provided with uninterrupted power sufficient to ensure the availability of repositories as specified in Section 2.2.1.

5.1.4 Water Exposures

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

5.1.5 Fire Prevention & 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 off-site 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

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 all uses of the DHS CAs and External CAs such as the FBCA or other External Entity CAs. 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 requirements of this policy are defined in terms of four principal roles. These four roles are employed at the CA, RA, and CSS locations as appropriate. (Note: This information derives from the *Certificate Issuing and Management Components (CIMC) Protection Profiles* [CIMC]):

1. *Administrator* – authorized to install, configure, and maintain the CA and CSS (where applicable); establish and maintain user accounts; configure profiles and audit parameters; and generate component keys;
2. *Officer* – authorized to request or approve certificates or certificate revocations;
3. *Auditor* – authorized to maintain audit logs; and
4. *Operator* – authorized to perform system backup and recovery.

Some principal roles may be combined. The principal roles required for each level of assurance are identified in Section 5.2.4.

The following subsections provide a detailed description of the responsibilities for each principal role.

5.2.1.1 Administrator

The administrator role is responsible for:

- Installation, configuration, and maintenance of the CA and CSS (where applicable);
- Establishing and maintaining CA and CSS system accounts;
- Configuring certificate profiles;
- Configuring CA, RA, and CSS audit parameters; and
- Generating and backing up CA and CSS keys.

Administrators do not issue certificates to Subscribers.

5.2.1.2 Officer

The officer role is responsible for issuing certificates, that is:

- Registering new Subscribers and requesting the issuance of certificates;
- Verifying the identity of Subscribers and accuracy of information included in certificates;
- Approving and executing the issuance of certificates, and;
- Requesting, approving and executing the revocation of certificates.

5.2.1.3 Auditor

The auditor role is responsible for:

- Reviewing, maintaining, and archiving audit logs; and
- Performing or overseeing internal compliance audits to ensure that the CA, associated RAs and CSS (if applicable) are operating in accordance with its CPS.

5.2.1.4 Operator

The operator role is responsible for the routine operation of the CA equipment and operations such as system backups and recovery or changing recording media.

5.2.1.5 Relationship Between Principal Roles and Other DHS PKI Roles

There are six DHS PKI trusted roles defined in Section 1.3.1, i.e., the DHS PKI Service Manager, the DHS PKI Policy Compliance Officer, the DHS PKI CA Key Custodian, the Registration Authority, the Local Registration Authority, and the Trusted Agent. The functions performed by all but one of these roles correspond to one of the Principal Roles in whole or in part, as shown in the following Table. Table entries indicate when the functions performed are a subset of the functions assigned to the Principal Role.

Relationship Between DHS PKI Roles	
Principal Role	**Other DHS PKI Trusted Roles**
Administrator	CA Key Custodian (Subset of Principal Role Functions)
Officer	Registration Authority
Officer	Local Registration Authority
Officer	Trusted Agent (Subset of Principal Role Functions)
Auditor	PKI Policy Compliance Officer

5.2.2 Number of Persons Required per Task

Only one person is required per task for CAs operating at the Rudimentary, Internal Basic and Basic Levels of Assurance.

Two or more persons are required for CAs operating at the Medium, Card Authentication, Medium Hardware, or High Levels of assurance for the following tasks:

- CA key generation;
- CA signing key activation;
- CA private key backup; and
- CA public key revocation.

Where multiparty control is required, at least one of the participants shall be an Administrator. All participants must serve in a trusted role as defined in Section 5.2.1. Multiparty control shall not be achieved using personnel that serve in the Auditor Trusted Role.

DHS employees appointed as DHS PKI CA Key Custodians (CAKC) shall control access to DHS CA keying materials containing DHS CA signing keys used to sign Medium, Card Authentication, Medium Hardware and High assurance certificates. The CAKC shall control access to DHS CA keying materials containing DHS CA signing keys, including all backups, from the time the keys are generated, until they are destroyed. This access control may be implemented as a multiparty control as long as an appointed CAKC is a mandatory participant.

A person in a trusted Role, whether enabled by the CA system or not, shall not approve or execute the issuance, renewal, or re-key of their own certificates. If circumstances prevent adherence to this rule, the action shall be documented and witnessed by another person in a Trusted Role and the documentation made part of the CA's official records.

5.2.3 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. At all assurance levels other than Rudimentary, an individual shall identify and authenticate him/herself before being permitted to perform any actions set forth above for that role or identity.

5.2.4 Separation of Roles

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

Requirements for the separation of roles, and limitations on use of procedural mechanisms to implement role separation, are described below for each level of assurance:

Assurance Level	Role Separation Rules
Rudimentary	No stipulation.
Internal Basic	Individual personnel shall be specifically designated to the four roles defined in Section 5.2.1 above. Individuals may assume more than one role. No individual shall be assigned more than one identity.
Basic	Individual personnel shall be specifically designated to the four roles defined in Section 5.2.1 above. Individuals may assume more than one role; however, no one individual shall assume both the Officer and Administrator roles. This may be enforced procedurally. No individual shall be assigned more than one identity.
Medium	Individual personnel shall be specifically designated to the four roles defined in Section 5.2.1 above. Individuals may only assume one of the Officer, Administrator, and Auditor roles, but any individual may assume the Operator role. The CA and RA software and hardware shall identify and authenticate its users and shall ensure that no user identity can assume both an Administrator and an Officer role, assume both the Administrator and Auditor roles, and assume both the Auditor and Officer roles. No individual shall have more than one identity.

Assurance Level	Role Separation Rules
Card Authentication	Individual personnel shall be specifically designated to the four roles defined in Section 5.2.1 above. Individuals may only assume one of the Officer, Administrator, and Auditor roles, but any individual may assume the Operator role. The CA and RA software and hardware shall identify and authenticate its users and shall ensure that no user identity can assume both an Administrator and an Officer role, assume both the Administrator and Auditor roles, and assume both the Auditor and Officer roles. No individual shall have more than one identity.
Medium Hardware	Individual personnel shall be specifically designated to the four roles defined in Section 5.2.1 above. Individuals may only assume one of the Officer, Administrator, and Auditor roles, but any individual may assume the Operator role. The CA and RA software and hardware shall identify and authenticate its users and shall ensure that no user identity can assume both an Administrator and an Officer role, assume both the Administrator and Auditor roles, and assume both the Auditor and Officer roles. No individual shall have more than one identity.
High	Individual personnel shall be specifically designated to the four roles defined in Section 5.2.1 above. Individuals may assume only one of the Officer, Administrator and Auditor roles. Individuals designated as Officer or Administrator may also assume the Operator role. An auditor may not assume any other role. The CA and RA software and hardware shall identify and authenticate its users and shall enforce these roles. No individual shall have more than one identity.

5.3 Personnel Controls

5.3.1 Background, Qualifications, Experience, & Security Clearance Requirements

The individual or group responsible and accountable for the operation of each CA or CSS in DHS is listed in the following table.

DHS CA	Responsible Individual or Group
Root CA	DHS PKI Policy Authority and DHS PKI Operational Authority
Medium Assurance CA for Internal Users	DHS PKI Policy Authority and DHS PKI

DHS CA	Responsible Individual or Group
	Operational Authority
Medium Assurance CA for Smart Cards	DHS PKI Policy Authority and DHS PKI Operational Authority

All persons filling trusted roles shall be selected on the basis of loyalty, trustworthiness, and integrity. For the DHS PKI, regardless of the assurance level, all trusted roles are required to be held by U.S. citizens. For DHS CAs operated at Medium Assurance and Medium Hardware, and associated CSSs, all trusted roles must be held by citizens of the country where the CA is located.

Where a DHS CA operated at Medium or Medium Hardware Assurance is affiliated with RAs operated overseas, RA personnel holding trusted roles may be local citizens of the country where the RA is located or of the country where the CA is located.

DHS PKI personnel acting in trusted roles shall hold SECRET security clearances.

5.3.2 Background Check Procedures

DHS PKI personnel acting in trusted roles shall, at a minimum, undergo background check procedures necessary to be cleared at the SECRET level.

DHS CA personnel shall, at a minimum, pass a background investigation covering the following areas:

- Employment;
- Education;
- Place of residence;
- Law Enforcement; and
- References.

The period of investigation must cover at least the last five years for each area, excepting the residence check which must cover at least the last three years. Regardless of the date of award, the highest educational degree shall be verified.

Adjudication of the background investigation shall be performed by a competent adjudication authority using a process consistent with Executive Order 12968 August 1995, or equivalent.

> Practice Note for federal agencies: A successfully adjudicated National Agency Check with Written Inquires (NACI) or National Agency Check with Law Enforcement Check (NACLC) on record is deemed to have met the minimum standards specified above.

In addition, DHS PKI personnel in trusted positions must:

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

5.3.3 Training Requirements

All personnel performing duties with respect to the operation of the DHS CAs or CSSs shall receive comprehensive training in all operational duties they are expected to perform, including disaster recovery and business continuity procedures.

In addition, personnel performing duties with respect to the operation of DHS CAs, the FBCA or other External Entity CAs shall receive comprehensive training, or demonstrate competence, in the following areas:

- CA/RA/CSS security principles and mechanisms; and
- All PKI software versions in use on the CA system.

Documentation shall be maintained identifying all personnel who received training and the level of training completed. Where competence was demonstrated in lieu of training, supporting documentation shall be maintained.

5.3.4 Retraining Frequency & Requirements

Individuals responsible for PKI roles shall be aware of changes in DHS CA and CSS 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 DHS CA software or hardware upgrade, changes in automated security systems, and relocation of equipment.

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

5.3.5 Job Rotation Frequency & Sequence

Any job rotation frequency and sequencing procedures shall provide for continuity and integrity of the DHS CA and CSS services.

5.3.6 Sanctions for Unauthorized Actions

The DHS PKI PA shall take appropriate actions where personnel have performed actions involving DHS CAs, their repositories, or CSSs not authorized in this CP, the applicable CPS, or other procedures published by the DHS PKI Operational Authority.

5.3.7 Independent Contractor Requirements

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

5.3.8 Documentation Supplied To Personnel

For DHS CAs and CSSs, documentation sufficient to define duties and procedures for each trusted role shall be provided to the personnel filling that role.

5.4 Audit Logging Procedures

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 *Retention Period For Archive*, Section 5.5.2.

5.4.1 Types of Events Recorded

A message from any source received by a DHS CA requesting an action related to the operational state of the CA is an auditable event. At a minimum, each audit record shall include the following (either recorded automatically or manually for each auditable event):

- The type of event;
- The date and time the event occurred;
- A success or failure indicator, where appropriate; and
- The identity of the entity and/or operator of the DHS CA that caused the event.

Detailed audit requirements are listed in the table below according to the level of assurance.

All security auditing capabilities of the DHS CA operating system and CA applications required by this CP shall be enabled. As a result, most of the events identified in the table shall be automatically recorded. Where events cannot be automatically recorded, the CA shall implement manual procedures to satisfy this requirement.

Auditable Event	**Assurance Level**						
	Rudimentary	**Internal Basic**	**Basic**	**Medium**	**Card Authentication**	**Medium Hardware**	**High**
SECURITY AUDIT							
Any changes to the Audit parameters, e.g., audit frequency, type of event audited		X	X	X	X	X	X

Auditable Event	**Assurance Level**						
	Rudimentary	**Internal Basic**	**Basic**	**Medium**	**Card Authentication**	**Medium Hardware**	**High**
Any attempt to delete or modify the Audit logs		X	X	X	X	X	X
Obtaining a third-party time-stamp		X	X	X	X	X	X
IDENTIFICATION AND AUTHENTICATION							
Successful and unsuccessful attempts to assume a role		X	X	X	X	X	X
The value of *maximum authentication attempts* is changed		X	X	X	X	X	X
The number of unsuccessful authentication attempts exceeds the *maximum authentication attempts* during user login		X	X	X	X	X	X
An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts		X	X	X	X	X	X
An Administrator changes the type of authenticator, e.g., from password to biometrics		X	X	X	X	X	X
LOCAL DATA ENTRY							
All security-relevant data that is entered in the system		X	X	X	X	X	X
REMOTE DATA ENTRY							
All security-relevant messages that are received by the system		X	X	X	X	X	X
DATA EXPORT AND OUTPUT							
All successful and unsuccessful requests for confidential and security-relevant information		X	X	X	X	X	X
KEY GENERATION							

Auditable Event	**Assurance Level**						
	Rudimentary	**Internal Basic**	**Basic**	**Medium**	**Card Authentication**	**Medium Hardware**	**High**
Whenever the CA generates a key. (Not mandatory for single session or one-time use symmetric keys)	X	X	X	X	X	X	X
PRIVATE KEY LOAD AND STORAGE							
The loading of Component private keys	X	X	X	X	X	X	X
All access to certificate subject private keys retained within the CA for key recovery purposes	X	X	X	X	X	X	X
TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE							
All changes to the trusted public keys, including additions and deletions	X	X	X	X	X	X	X
SECRET KEY STORAGE							
The manual entry of secret keys used for authentication				X	X	X	X
PRIVATE AND SECRET KEY EXPORT							
The export of private and secret keys (keys used for a single session or message are excluded)	X	X	X	X	X	X	X
CERTIFICATE REGISTRATION							
All certificate requests	X	X	X	X	X	X	X
CERTIFICATE REVOCATION							
All certificate revocation requests		X	X	X	X	X	X
CERTIFICATE STATUS CHANGE APPROVAL							
The approval or rejection of a certificate status change request		X	X	X	X	X	X
CA CONFIGURATION							
Any security-relevant changes to the configuration of the CA		X	X	X	X	X	X

Auditable Event	Assurance Level						
	Rudimentary	Internal Basic	Basic	Medium	Card Authentication	Medium Hardware	High
ACCOUNT ADMINISTRATION							
Roles and users are added or deleted	X	X	X	X	X	X	X
The access control privileges of a user account or a role are modified	X	X	X	X	X	X	X
CERTIFICATE PROFILE MANAGEMENT							
All changes to the certificate profile	X	X	X	X	X	X	X
REVOCATION PROFILE MANAGEMENT							
All changes to the revocation profile		X	X	X	X	X	X
CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT							
All changes to the certificate revocation list profile		X	X	X	X	X	X
MISCELLANEOUS							
Appointment of an individual to a Trusted Role	X	X	X	X	X	X	X
Designation of personnel for multiparty control				X	X	X	X
Installation of the Operating System		X	X	X	X	X	X
Installation of the CA		X	X	X	X	X	X
Installing hardware cryptographic modules				X	X	X	X
Removing hardware cryptographic modules				X	X	X	X
Destruction of cryptographic modules		X	X	X	X	X	X
System Startup		X	X	X	X	X	X
Logon Attempts to CA Applications		X	X	X	X	X	X
Receipt of Hardware/Software				X	X	X	X
Attempts to set passwords		X	X	X	X	X	X

Auditable Event	**Assurance Level**						
	Rudimentary	**Internal Basic**	**Basic**	**Medium**	**Card Authentication**	**Medium Hardware**	**High**
Attempts to modify passwords		X	X	X	X	X	X
Backing up CA internal database		X	X	X	X	X	X
Restoring CA internal database		X	X	X	X	X	X
File manipulation (e.g., creation, renaming, moving)				X	X	X	X
Posting of any material to a repository				X	X	X	X
Access to CA internal database				X	X	X	X
All certificate compromise notification requests		X	X	X	X	X	X
Loading tokens with certificates				X	X	X	X
Shipment of Tokens				X	X	X	X
Zeroizing tokens		X	X	X	X	X	X
Re-key of the CA	X	X	X	X	X	X	X
Configuration changes to the CA server involving:							
- Hardware		X	X	X	X	X	X
- Software		X	X	X	X	X	X
- Operating System		X	X	X	X	X	X
- Patches		X	X	X	X	X	X
- Security Profiles				X	X	X	X
PHYSICAL ACCESS / SITE SECURITY							
Personnel Access to room housing CA				X	X	X	X
Access to the CA server				X	X	X	X
Known or suspected violations of physical security		X	X	X	X	X	X
ANOMALIES							

Auditable Event	Assurance Level						
	Rudimentary	Internal Basic	Basic	Medium	Card Authentication	Medium Hardware	High
Software Error conditions		X	X	X	X	X	X
Software check integrity failures		X	X	X	X	X	X
Receipt of improper messages				X	X	X	X
Misrouted messages				X	X	X	X
Network attacks (suspected or confirmed)		X	X	X	X	X	X
Equipment failure	X	X	X	X	X	X	X
Electrical power outages				X	X	X	X
Uninterruptible Power Supply (UPS) failure				X	X	X	X
Obvious and significant network service or access failures				X	X	X	X
Violations of Certificate Policy	X	X	X	X	X	X	X
Violations of Certification Practice Statement	X	X	X	X	X	X	X
Resetting Operating System clock		X	X	X	X	X	X

5.4.2 Frequency of Processing Log

Audit logs shall be reviewed in accordance to the table below. Such reviews involve verifying that the log has not been tampered with, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities (e.g., discontinuities in the logs and loss of audit data) in the log. Actions taken as a result of these reviews shall be documented.

For the DHS Root CA, the DHS PKI Operational Authority shall explain all significant events in an audit log summary.

Assurance Level	Review Audit Log
Rudimentary	Only required for cause

Assurance Level	Review Audit Log
Internal Basic	Only required for cause
Basic	Only required for cause
Medium	At least once every two months Statistically significant set of security audit data generated by DHS CAs since the last review shall be examined (where the confidence intervals for each category of security audit data are determined by the security ramifications of the category and the availability of tools to perform such a review), as well as a reasonable search for any evidence of malicious activity
Card Authentication	At least once every two months Statistically significant set of security audit data generated by DHS CAs since the last review shall be examined (where the confidence intervals for each category of security audit data are determined by the security ramifications of the category and the availability of tools to perform such a review), as well as a reasonable search for any evidence of malicious activity
Medium Hardware	At least once every two months Statistically significant set of security audit data generated by DHS CAs since the last review shall be examined (where the confidence intervals for each category of security audit data are determined by the security ramifications of the category and the availability of tools to perform such a review), as well as a reasonable search for any evidence of malicious activity
High	At least once per month Statistically significant set of security audit data generated by DHS CAs since the last review shall be examined (where the confidence intervals for each category of security audit data are determined by the security ramifications of the category and the availability of tools to perform such a review), as well as a reasonable search for any evidence of malicious activity

5.4.3 Retention Period for Audit Logs

For Medium, Card Authentication, Medium Hardware, and High Assurance, audit logs shall be retained on-site until reviewed, as well as being retained in the manner described below. For Rudimentary, Internal Basic and Basic Assurance, audit logs shall be retained on-site for at least two months or until reviewed, as well as being retained in the manner described below. The individual who removes audit logs from the DHS CA system shall be an official different from the individuals who, in combination, command the DHS CA signature key.

5.4.4 Protection of Audit Logs

DHS CA system configuration and procedures must be implemented together to ensure that:

- Only personnel assigned to trusted roles have read access to the logs;
- Only authorized people may archive audit logs; and,
- Audit logs are not modified.

The entity performing audit log archive need not have modify access, but procedures must be implemented to protect archived data from destruction prior to the end of the audit log retention period (note that deletion requires modification access).

The off-site storage location for audit logs shall be a safe, secure location separate from the CA equipment.

Audit data generated in hardcopy form shall be copied and stored in a safe, secure location separate from the CA equipment.

Practice Note: If a system over-writes audit logs after a given time, the audit log is not considered deleted or destroyed if the audit log has been backed up and archived.

5.4.5 Audit Log Backup Procedures

Audit logs and audit summaries shall be backed up at least monthly. A copy of the audit log shall be sent off-site on a monthly basis and stored in a safe, secure location separate from the CA equipment.

5.4.6 Audit Collection System

The audit log collection system may or may not be external to the DHS CA system. Automated audit processes shall be invoked at system (or application) startup, and cease only at system (or application) shutdown. Should it become apparent that an automated audit system has failed, and the integrity of the system or confidentiality of the information protected by the system is at risk, then the DHS PKI OA shall determine whether to suspend DHS CA operation until the problem is remedied.

5.4.7 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.

5.4.8 Vulnerability Assessments

DHS CA personnel shall routinely assess security controls for vulnerabilities, look for evidence of malicious activities, and access whether the CA system or its components have been attacked or breached.

Practice Note: The audit logs shall be checked for anomalies in support of any suspected violation.

Practice Note: The audit logs shall be reviewed for events such as repeated failed actions, requests for privileged information, attempted access of system files, and unauthenticated responses. Checks shall also check for continuity of the audit logs.

5.5 Records Archive

5.5.1 Types of Events Archived

DHS CA archive records shall be sufficiently detailed 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 recorded for archive in accordance with each assurance level:

Data To Be Archived	Assurance Level						
	Rudimentary	Internal Basic	Basic	Medium	Card Authentication	Medium Hardware	High
CA accreditation (if applicable)	X	X	X	X	X	X	X
Certification Practice Statement	X	X	X	X	X	X	X
Contractual obligations	X	X	X	X	X	X	X
System and equipment configuration	X	X	X	X	X	X	X
Modifications and updates to system or configuration	X	X	X	X	X	X	X
Certificate requests	X	X	X	X	X	X	X
Revocation requests		X	X	X	X	X	X

Data To Be Archived	**Assurance Level**						
	Rudimentary	**Internal Basic**	**Basic**	**Medium**	**Card Authentication**	**Medium Hardware**	**High**
Subscriber identity authentication data as per Section 3.1.9			X	X	X	X	X
Documentation of receipt and acceptance of certificates			X	X	X	X	X
Documentation of receipt of tokens			X	X	X	X	X
All certificates issued or published	X	X	X	X	X	X	X
Record of CA Re-key	X	X	X	X	X	X	X
All CRLs issued and/or published		X	X	X	X	X	X
All Audit Logs	X	X	X	X	X	X	X
Other data or applications to verify archive contents		X	X	X	X	X	X
Documentation required by compliance auditors			X	X	X	X	X

5.5.2 Retention Period for Archive

The minimum retention periods for archive data are identified below. DHS must follow either the General Records Schedule established by the National Archives and Records Administration or a DHS-specific schedule as applicable.

This minimum retention period for these records is intended only to facilitate the operation of the DHS CAs.

Assurance Level	**Minimum Retention Period**
Rudimentary	7 Years & 6 Months

Assurance Level	Minimum Retention Period
Internal Basic	As Specified in CPS
Basic	7 Years & 6 Months
Card Authentication	10 Years & 6 Months
Medium	10 Years & 6 Months
Medium Hardware	10 Years & 6 Months
High	20 Years & 6 Months

5.5.3 Protection of Archive

No unauthorized user shall be permitted to write to or delete the archive. For DHS CAs, archived records may be moved to another medium when authorized by the DHS PKI OA. Archive media shall be stored in a safe, secure storage facility separate from the DHS CA itself.

If the original 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.

Alternatively, a DHS CA may retain data using whatever procedures have been approved by NARA for that category of documents. Applications required to process the archive data shall also be maintained for a period determined by the DHS PKI PA for DHS CAs.

Prior to the end of the archive retention period, the DHS PKI OA shall provide archived data and the applications necessary to read the archives to an archival facility approved by the DHS PKI PA for long term storage. This facility shall retain the applications necessary to read this archived data.

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

5.5.4 Archive Backup Procedures

The CPS for each DHS CA or a referenced document shall describe how archive records are backed up, and how the archive backups are managed.

5.5.5 Requirements for Time-Stamping of Records

DHS CA archive records shall be automatically time-stamped as they are created. The CPS for the CA shall describe how system clocks used for time-stamping are maintained in synchrony with an authoritative time standard.

5.5.6 Archive Collection System (Internal or External)

No stipulation.

5.5.7 Procedures to Obtain & Verify Archive Information

Each DHS CA shall publish in its CPS procedures detailing how to create, verify, package, transmit, and store archive information.

The contents of the archive shall not be released except as determined by the DHS PKI PA or 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.

5.6 Key Changeover

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, public key 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 cover certificates signed with that key, then the old key must be retained and protected.

The DHS Root CA shall implement key changeover procedures that establish key certificates, where a certificate containing the old public key will be signed by the new private key, and a certificate containing the new public key will be signed by the old private key.

When a DHS Subordinate CA implements a key changeover, the Subordinate CA must obtain a new certificate for the new public key from the DHS Root CA.

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

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

DHS CAs must re-key-before their private signing keys exceed their maximum usage period, as specified in their CPS.

Section 6.3.2 identifies maximum time limitations on the use of private keys and their associated public keys (certificate validity periods) for the DHS PKI.

5.7 Compromise & Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

The DHS PKI PA shall be notified by the DHS PKI OA if any of the following situations occur:

- Suspected or detected compromise of DHS CA systems;
- Suspected or detected compromise of a Certificate Status Server (CSS) if (1) the CSS certificate has a lifetime of more than 72 hours and (2) the CSS certificate cannot be revoked (e.g., an OCSP server certificate with the no-check extension);

- Physical or electronic attempts to penetrate DHS CA systems;
- Denial of service attacks on DHS CA components; and
- Any incident preventing a DHS CA from issuing a CRL within 24 hours of the time specified in the next update field of its currently valid CRL.

The DHS PKI PA shall notify the FPKIPA, FBCA and External Entity CAs cross certified with the DHS PKI as required by the applicable MOA. Internal relying parties shall be notified as determined by the DHS PKI PA.

The DHS PKI OA shall reestablish operational capabilities as quickly as possible in accordance with procedures set forth in the governing CPSs for the effected DHS CAs. 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.

5.7.2 Computing Resources, Software, and/Or Data Are Corrupted

When computing resources, software, and/or data are corrupted, the DHS CAs shall respond as follows:

- If the CA signature keys are not destroyed**,** CA operation shall be reestablished, giving priority to the ability to generate certificate status information within the CRL issuance schedule specified in 4.9.7, Table 1; and
- If the CA signature keys are destroyed**,** CA operation shall be reestablished as quickly as possible, giving priority to the generation of a new CA key pair.

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.

5.7.3 DHS CA Private Key Compromise Procedures

If a DHS CA’s signature keys are compromised or lost (such that compromise is possible even though not certain):

- The DHS PKI PA shall notify the FPKIPA, FBCA and External Entity CAs cross certified with the DHS PKI so that they may issue CRLs revoking any cross-certificates issued to the compromised DHS CA;
- A new DHS CA key pair shall be generated by the CA in accordance with procedures set forth in the DHS CA’s CPS;
- If the CA is the DHS Root CA, the trusted self-signed certificate shall be removed from each relying party application, and a new one distributed, via secure out-of-band mechanisms. The Root CA CPS shall define the process to be followed in the event of Root CA key compromise.

- If the CA is a Subordinate CA, the DHS Root CA shall revoke the compromised CA's certificate and the revocation information shall be published immediately in the most expedient manner. The DHS Root CA shall sign the certificate for the new Subordinate CA's signing key pair.
- The CA shall re-issue cross certificates, CA certificates and Subscriber certificates under its new signing key in accordance with the CA's CPS.

The DHS PKI PA shall also investigate and report to the Federal PKI Policy Authority what caused the compromise or loss, and what measures have been taken to preclude recurrence.

In case of a CSS key compromise, the CA that issued the CSS certificate, shall revoke that CSS's certificate, and the revocation information shall be published immediately. Subsequently, the CSS shall be re-keyed. If the CSS 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 CSS CPS shall describe the approach to reacting to a CSS key compromise.

5.7.4 Business Continuity Capabilities after a Disaster

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

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

The DHS PKI OA shall operate one or more backup sites, whose purpose is to ensure continuity of operations in the event of failure of a primary site. DHS CA operations shall be designed to restore full service as quickly as feasible after primary system failure.

The DHS PKI PA shall at the earliest feasible time securely advise the Federal PKI Policy Authority and all of its member entities in the event of a disaster where the DHS Root CA installation is physically damaged and all copies of the Root CA signature keys are destroyed.

Relying Parties may decide of their own volition whether to continue to use certificates signed with the destroyed private key pending reestablishment of DHS CA operation with new certificates.

5.8 CA & RA Termination

In the event that a DHS CA terminates operations, certificates signed by the CA shall be revoked. The DHS PKI PA shall advise the Federal PKI Policy Authority and other External Entities that are cross certified with the DHS CA and have entered into MOAs with the DHS PKI PA that the DHS CA's operations will be terminated so they may revoke certificates they have issued to the DHS CA. The notification shall be provided prior to termination.

Reasonable efforts shall be made to promptly notify Subscribers and other relying parties. Entities will be given as much advance notice as circumstances permit.

The DHS PKI OA shall provide all archived data and records for the terminated CA to an archival facility at termination of operations.

6.0 TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation & Installation

6.1.1 Key Pair Generation

6.1.1.1 CA Key Pair Generation

Cryptographic keying material used to sign certificates, CRLs or status information by a DHS CA shall be generated in FIPS 140 validated cryptographic modules.

For DHS CAs, the modules shall meet or exceed Security Level 1 (for Rudimentary), Security Level 2 (for Internal Basic or Basic), or Security Level 3 (for Medium, Card Authentication, Medium Hardware or High). Multiparty control is required for CA key pair generation DHS CAs operating at the Medium, Card Authentication, Medium Hardware, or High levels of assurance, as specified in Section 5.2.2.

CA key pair generation must create a verifiable audit trail that the security requirements for procedures were followed. For all levels of assurance, the documentation of the procedure must be detailed enough to show that appropriate role separation was used.

Practice Note: If the audit trail identifies and documents any failures or anomalies in the key generation process, along with the corrective action taken, the key generation process need not be restarted but may continue.

For High, Medium Hardware, Card Authentication, and Medium the process shall be validated by an independent third party.

6.1.1.2 Subscriber Key Pair Generation

Subscriber key pair generation may be performed by the Subscriber, the authorized Sponsor for a non-human Subscriber, CA, or RA. If the authorized Sponsor for a non-human Subscriber, CA or RA generates Subscriber key pairs, the requirements for key pair delivery specified in Section 6.1.2 must also be met.

Key generation shall be performed using a FIPS approved method.

At the High, Medium Hardware and Card Authentication assurance levels, Subscriber key generation must be performed using a FIPS 140 Level 2 hardware cryptographic module. For all other assurance levels, either software or hardware cryptographic modules may be used for key generation.

6.1.2 Private Key Delivery to Subscriber

If Subscribers generate their own key pairs, then there is no need to deliver private keys, and this section does not apply.

When authorized Sponsors for a non-human Subscribers, CAs or RAs generate keys on behalf of the Subscriber, then the private key must be delivered securely to the Subscriber. Private keys may be delivered electronically or may be delivered on a hardware cryptographic module. In all cases, the following requirements must be met:

- Anyone who generates a private signing key for a Subscriber shall not retain any copy of the key after delivery of the private key to the Subscriber;
- The private key must be protected from activation, compromise, or modification during the delivery process;
- The Subscriber, or Sponsor receiving a key on behalf of a non-human Subscriber, shall acknowledge receipt of the private key(s); and
- Delivery shall be accomplished in a way that ensures that the correct tokens and activation data are provided to the correct Subscribers:
  - For hardware modules, accountability for the location and state of the module must be maintained until the Subscriber, or Sponsor receiving a key on behalf of a non-human Subscriber, accepts possession of it;
  - For electronic delivery of private keys, the key material shall be encrypted using a cryptographic algorithm and key size at least as strong as the private key. Activation data shall be delivered using a separate secure channel; and
  - For shared key applications, organizational identities, and devices, see also Section 3.2.

The DHS CA must maintain a record of the Subscriber’s acknowledgement of receipt of the token.

6.1.3 Public Key Delivery to Certificate Issuer

For DHS CAs operating at the Basic, Medium, Card Authentication, Medium Hardware, or High level of assurance, the following requirements apply:

- Where key pairs are generated by the Subscriber, authorized Sponsor for a non-human Subscriber, or RA, the public key and the Subscriber’s identity must be delivered securely to the CA for certificate issuance; and
- The delivery mechanism shall bind the Subscriber’s verified identity to the public key. If cryptography is used to achieve this binding, it must be at least as strong as the CA keys used to sign the certificate.

For DHS CAs operating at the Rudimentary or Internal Basic level of assurance, the requirements for public key delivery to the certificate issuer shall be specified in the governing CPS.

6.1.4 CA Public Key Delivery to Relying Parties

When a CA updates its signature key pair, the CA shall distribute the new public key in a secure fashion. The new public key may be distributed in a self-signed certificate, in a key rollover certificate, or in a new CA (e.g., cross-certificate or subordinate CA certificate) certificate obtained from the issuer(s) of the current CA certificate(s).

Self-signed certificates shall be conveyed to relying parties in a secure fashion to preclude substitution attacks.

Practice Note: Known acceptable methods for self-signed certificate delivery include:

- *The CA loading a self-signed certificate onto tokens delivered to Relying Parties via secure mechanisms;*
- *Secure distribution of self-signed certificates through secure out-of-band mechanisms;*
- *Comparison of the hash of the self-signed certificate against a hash value made available via authenticated out-of-band sources (note that hashes posted in-band along with the certificate are not acceptable as an authentication mechanism); and*
- *Loading certificates from web sites secured with a currently valid certificate of equal or greater assurance level than the certificate being downloaded.*

Other methods that preclude substitution attacks may be considered acceptable.

Key rollover certificates are signed with the CA's current private key, so secure distribution is not required.

CA Certificates are signed with the issuing CA's current private key, so secure distribution is not required.

6.1.5 Key Sizes

All FIPS-approved signature algorithms shall be considered acceptable; additional restrictions on key sizes are detailed below.

For CAs that distribute self-signed certificates to relying parties, the CA's subject public keys in such certificates shall be at least 2048 bits for RSA, or at least 224 bits for ECDSA.

CAs that generate certificates and CRLs under this policy shall use signature keys of at least 1024 bits for RSA or DSA, and at least 160 bits for ECDSA. Certificates that expire after 12/31/08 shall be generated with at least 2048 bit RSA key, or at least 224 bits for ECDSA.

CAs that generate certificates and CRLs under this policy shall use SHA-1, SHA-224, SHA-256, SHA-384, or SHA-512 hash algorithm when generating digital signatures. Signatures on certificates and CRLs that are issued after 12/31/08 shall be generated using, at a minimum, SHA-224.

Where implemented, CSSs shall sign responses using the same signature algorithm, key size, and hash algorithm used by the CA to sign CRLs.

End-entity certificates that expire before 12/31/08 shall contain public keys that are at least 1024 bit for RSA, DSA, or Diffie-Hellman, or 160 bits for elliptic curve algorithms. End-entity certificates that expire on or after 12/31/08 shall contain public keys that are at least 2048 bit for RSA or Diffie-Hellman, or 224 bits for elliptic curve algorithms.

Use of TLS or another protocol providing similar security to accomplish any of the requirements of this CP shall require at a minimum triple-DES or equivalent for the symmetric key, and at least 1024 bit RSA or equivalent for the asymmetric keys through 12/31/08. Use of TLS or another protocol providing similar security to accomplish any of the requirements of this CP shall require at a minimum AES (128 bits) or equivalent for the symmetric key, and at least 2048 bit RSA or equivalent for the asymmetric keys after 12/31/08.

6.1.6 Public Key Parameters Generation and Quality Checking

Public key parameters for signature algorithms defined in the *Digital Signature Standard (DSS)* [FIPS 186-2] shall be generated in accordance with FIPS 186-2.

Parameter quality checking (including primarily testing for prime numbers) shall be performed in accordance with FIPS 186; additional tests may be specified by the Federal PKI Policy Authority.

6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)

Public keys that are bound into certificates shall be certified for use in signing or encrypting, but not both, except as specified below. The use of a specific key is determined by the key usage extension in the X.509 certificate.

CA certificates issued by DHS CAs shall set two key usage bits: *cRLSign* and/or *keyCertSign*. Where the subject signs OCSP responses, the certificate may also set the *digitalSignature* and/or *nonRepudiation* bits.

Subscriber certificates shall assert key usages based on the intended application of the key pair. In particular:

- Certificates to be used only for authentication shall set the *digitalSignature* bit;
- Certificates to be used for digital signatures (including authentication) shall set the *digitalSignature* and/or *nonRepudiation* bits;
- Certificates to be used for key or data encryption shall set the *keyEncipherment* and/or *dataEncipherment* bits; and
- Certificates to be used for key agreement shall set the *keyAgreement* bit.

DHS Subscriber keys shall not be certified for use in both signing and encrypting, with the following exception:

- Rudimentary, Basic, and Medium Assurance Level certificates may include a single key for use with encryption and signature in support of legacy applications. Such dual-use certificates shall be generated and managed in accordance with their respective signature certificate requirements, except where otherwise noted in this CP. Such dual-use certificates shall never assert the non-repudiation key usage bit, and shall not be used for authenticating data that will be verified on the basis of the dual-use certificate at a future time.

6.2 Private Key Protection & Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards & Controls

The relevant standard for cryptographic modules is FIPS PUB 140, *Security Requirements for Cryptographic Modules*.

Cryptographic modules shall be validated to the FIPS 140 level identified in this section. Additionally, the DHS PKI PA reserves the right to review technical documentation associated with any cryptographic modules under consideration for use by a DHS CA.

The table below summarizes the minimum requirements for cryptographic modules; higher levels may be used.

Assurance Level	CA	Subscriber	RA
Rudimentary	Level 1 (Hardware or Software)	N/A	Level 1 (Hardware or Software)
Internal Basic	Level 2 (Hardware)	Level 1	Level 1 (Hardware or Software)
Basic	Level 2 (Hardware)	Level 1	Level 1 (Hardware or Software)
Medium	Level 3 (Hardware)	Level 1	Level 2 (Hardware)
Card Authentication	Level 3 (Hardware)	Level 2 (Hardware)	Level 2 (Hardware)
Medium Hardware	Level 3 (Hardware)	Level 2 (Hardware)	Level 2 (Hardware)
High	Level 3 (Hardware)	Level 2 (Hardware)	Level 2 (Hardware)

6.2.2 Private Key Multi-Person Control

Use of the DHS Root CA private signing key shall require action by multiple persons as set forth in Section 5.2.2 of this CP.

Use of other DHS CA private signing keys shall require action by multiple persons at Medium, Card Authentication, Medium Hardware, and High Assurance as set forth in Section 5.2.2 of this CP.

6.2.3 Private Key Escrow

6.2.3.1 Escrow of CA Private Signature Key

Under no circumstances shall a DHS CA signature key used to sign certificates or CRLs be escrowed.

6.2.3.2 Escrow of CA Encryption Keys

No stipulation.

6.2.3.3 Escrow of Subscriber Private Signature Keys

Subscriber private signature keys shall not be escrowed.

6.2.3.4 Escrow of Subscriber Private Encryption and Dual Use Keys

Subscriber private dual use keys shall not be escrowed.

All Subscriber private encryption keys shall be escrowed by the CA issuing the Subscriber's certificate, or by some other trusted escrow system, as described in Section 4.12.1 and in the CA's CPS.

6.2.4 Private Key Backup

6.2.4.1 Backup of DHS CA Private Signature Key

Backup of DHS CA private signature keys is required to facilitate disaster recovery.

DHS CA private signature keys shall be backed up under multi-person control, as specified in Section 5.2.2.

Access to backup copies of DHS CA private signature keys shall be controlled as specified in Section 5.2.2.

No more than a single copy of the signature key shall be stored at the operational site of the CA. However, if a copy of the signature key plus the original key are used together in a high-availability CA configuration, two copies of the CA signing key may be stored at the operational site of the CA.

Additional copies may exist off-site provided that accountability for them is maintained.

All copies of the signature key must be 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 Key

At the Card Authentication, Medium Hardware and High assurance levels, Subscriber private signature keys may not be backed up or copied.

At the Rudimentary, Internal Basic, Basic, or Medium levels of assurance, Subscriber private signature keys 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.

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 non-human Subscribers, 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 signature keys shall not be archived.

The private decryption keys shall be encrypted and delivered to the key recovery mechanism associated with the issuing 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 5.5.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

DHS CA private keys shall be generated by and remain in a cryptographic module. The CA private keys may be backed up in accordance with Section 6.2.4.1.

Subscriber private keys shall be generated by and remain in a cryptographic module. Subscriber private keys may be backed up in accordance with Section 6.2.4.2.

6.2.7 Private Key Storage on Cryptographic Module

No stipulation.

6.2.8 Method of Activating Private Keys

For DHS CAs that operate at the Medium, Card Authentication, Medium Hardware, or High level of assurance, CA signing key activation requires multiparty control as specified in Section 5.2.2.

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).

For certificates issued under Card Authentication, Cardholder authentication is not required to use the associated private key.

6.2.9 Methods of Deactivating Private Keys

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. Cryptographic modules containing DHS CA private signing keys shall remain under the control of an appointed DHS employee at all times, as specified in Section 5.2.2.

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.

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.

6.2.10 Method of Destroying Subscriber Private Signature Keys

Individuals in trusted roles shall destroy CA, RA and status server (e.g., OCSP server) private signature keys when they are no longer needed. 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 accomplished by overwriting the data using an authorized utility. For hardware cryptographic modules, this will likely be accomplished by executing a “zeroize” command. Physical destruction of hardware is not required.

6.2.11 Cryptographic Module Rating

See Section 6.2.1

6.3 Other Aspects Of Key Management

6.3.1 Public Key Archival

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

6.3.2 Certificate Operational Periods/Key Usage Periods

CAs use their signing keys for certificate and CRL signing functions.

CAs must 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 Subordinate CAs and Subscribers.

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

PIV authentication certificates must expire no later than the PIV card expiration date.

PIV card authentication certificates must expire no later than the PIV card expiration date.

PIV optional digital signature certificates must expire no later than the PIV card expiration date.

PIV content signing certificates should not expire before the PIV card expires.

The validity period of Subscriber certificates must not exceed the routine re-key Identity Requirements as specified in Section 3.3.1.

CAs must not issue cross certificates that extend beyond the period of the governing MOA.

The following table identifies maximum time limitations on the use of private keys and their associated public keys (certificate validity periods) for the DHS PKI. Each DHS PKI CA shall specify private and public key certificate usage periods for the certificates it issues in the governing CPS.

Entity	Private Key Use	Limitation on Private Key Usage	Limitation on Public Key Usage
DHS Root CA	Signing Self-signed Certificate (used as Trust Anchor)	Maximum of 10 Years	Maximum of 20 Years
All Other DHS CAs	Signing Subscriber Certificates	Maximum of 4 Years	
	Signing OCSP Responder Certificates	Maximum of 10 Years	
	Signing CRLs	Maximum of 10 Years	
Code Signer	Signing Code	Maximum of 3 Years	Not to Exceed 8 Years
Content Signer	Signing Content	Maximum of 3 Years	Not to Exceed 8 Years
Subscriber	Signing	Maximum of 3 Years	Maximum of 3 Years
	Key Management	Unrestricted	Maximum of 3 Years

Practice Note: Signatures generated with the private key may be validated after expiration of the public key certificate.

Each DHS PKI CA shall specify the certificate lifetimes and key usage periods it employs in the applicable CPS.

6.4 Activation Data

6.4.1 Activation Data Generation & Installation

The activation data used to unlock DHS 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. 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. Where passwords are used for activation, they shall be generated in conformance with FIPS 112. Where the DHS CA uses passwords as activation data for the CA signing key, at a minimum the activation data shall be changed upon CA re-key.

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 be:

- Memorized;
- Biometric in nature; or
- If written down, recorded and secured at the level of assurance associated with the activation of the cryptographic module, and shall not be stored with the cryptographic module.

The protection mechanism shall include a facility to temporarily lock the account, or terminate the application, after a predetermined number of failed login attempts as set forth 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

For the DHS Root CA, the computer security functions listed below are required. These functions may be provided by the operating system, or through a combination of operating system, software, and physical safeguards. The DHS Root CA and its ancillary parts shall include the following functionality:

- Require authenticated logins;
- Provide Discretionary Access Control;
- Provide a security audit capability;
- Restrict access control to CA services and PKI roles;
- Enforce separation of duties for PKI roles;
- Require identification and authentication of PKI roles and associated identities;
- Prohibit object re-use or require separation for CA random access memory;
- Require use of cryptography for session communication and database security;
- Archive CA history and audit data;
- Require self-test security related CA services;
- Require a trusted path for identification of PKI roles and associated identities;

- Require a recovery mechanisms for keys and the CA system;
- Enforce domain integrity boundaries for security critical processes; and
- Support recovery from key or system failure.

For other DHS CAs, the computer security functions listed below are required. These functions may be provided by the operating system, or through a combination of operating system, software, and physical safeguards. The DHS Subordinate CAs and their ancillary parts shall include the following functionality:

- Authenticate the identity of users before permitting access to the system or applications;
- Manage privileges of users to limit users to their assigned roles;
- Generate and archive audit records for all transactions (See Section 5.4);
- Enforce domain integrity boundaries for security critical processes; and
- Support recovery from key or system failure.

For Certificate Status Servers operating under this policy, the computer security functions listed below are required:

- Authenticate the identity of users before permitting access to the system or applications;
- Manage privileges of users to limit users to their assigned roles;
- Enforce domain integrity boundaries for security critical processes; and
- Support recovery from key or system failure.

6.5.2 Computer Security Rating

No Stipulation.

6.6 Life-Cycle Security Controls

6.6.1 System Development Controls

The System Development Controls for DHS CAs at the Internal Basic, Basic, Medium, Card Authentication, Medium Hardware and High Assurance levels are as follows:

- For commercial off-the-shelf software, the software shall be designed and developed under a formal, documented development methodology;
- For hardware and software developed specifically for a particular CA, the applicant shall demonstrate that security requirements were achieved through a combination of software verification & validation, structured development approach, and controlled development environment;
- Where open source software has been utilized, the applicant shall demonstrate that security requirements were achieved through software verification & validation and structured development/life-cycle management;

- Hardware and software procured to operate the CA shall be purchased and shipped in a fashion to reduce the likelihood that any particular component was tampered with (e.g., by ensuring the equipment was randomly selected at time of purchase);
- The CA hardware and software shall be dedicated to performing one task: the CA. There shall be no other applications; hardware devices, network connections, or component software installed which are not part of the CA operation;
- Proper care shall be taken to prevent malicious software from being loaded onto the CA equipment. Hardware and software shall be scanned for malicious code on first use and periodically thereafter; and
- Hardware and software 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.

6.6.2 Security Management Controls

The configuration of DHS CA systems as well as any modifications and upgrades shall be documented and controlled. There shall be a mechanism for detecting unauthorized modification to the CA software or configuration. A formal configuration management methodology shall be used for installation and ongoing maintenance of the DHS CA system. The DHS CA 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 DHS CA software shall be verified by the DHS PKI OA at least monthly.

6.6.3 Life Cycle Security Ratings

No stipulation.

6.7 Network Security Controls

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

The DHS Border Directory shall be connected to the Internet and provide continuous service (except, when necessary, for brief periods of maintenance or backup).

6.8 Time Stamping

Asserted times shall be accurate to within three minutes. Electronic or manual procedures may be used to maintain system time. Clock adjustments are auditable events, see Section 5.4.1.

7.0 CERTIFICATE, CARL/CRL, AND OCSP PROFILES FORMAT

7.1 Certificate Profile

7.1.1 Version Numbers

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

7.1.2 Certificate Extensions

For all CAs, use of standard certificate extensions shall comply with [RFC 3280].

Certificates issued by DHS CAs shall comply with the ***Federal Public Key Infrastructure X.509 Certificate and CRL Extensions Profile*** [FPKI-PROF].

CA Certificates issued by the DHS CAs shall not include critical private extensions.

Subscriber certificates issued by DHS CAs may include critical private extensions so long as interoperability within the community of use is not impaired. Whenever private extensions are used, they shall be identified in the applicable CPS.

7.1.3 Algorithm Object Identifiers

Certificates issued by DHS CAs shall identify the signature algorithm using one of the following OIDs:

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 }
id-RSASSA-PSS	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 10 }
ecdsa-with-SHA1	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) 1 }
ecdsa-with-SHA224	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 1 }
ecdsa-with-SH256	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2 (3) 2 }
ecdsa-with-SHA384	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 3 }
ecdsa-with-SHA512	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 4 }

Where certificates are signed using RSA with PSS padding, the OID is independent of the hash algorithm; the hash algorithm is specified as a parameter. RSA signatures with PSS padding may be used with the hash algorithms and OIDs specified below:

id-sha256	{ joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 1 }
id-sha512	{ joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 3 }

Certificates issued by DHS CAs shall identify the cryptographic algorithm associated with the subject public key using one of the following OIDs:

id-dsa	{ iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 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-ecPublicKey	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) id-publicKeyType(2) 1 }

Where non-CA certificates issued on behalf of federal agencies contain an elliptic curve public key, the parameters shall be specified as one of the following named curves:

ansip192r1	{ iso(1) member-body(2) us(840) 10045 curves(3) prime(1) 1 }
ansit163k1	{ iso(1) identified-organization(3) certicom(132) curve(0) 1 }
ansit163r2	{ iso(1) identified-organization(3) certicom(132) curve(0) 15 }
ansip224r1	{ iso(1) identified-organization(3) certicom(132) curve(0) 33 }
ansit233k1	{ iso(1) identified-organization(3) certicom(132) curve(0) 26 }
ansit233r1	{ iso(1) identified-organization(3) certicom(132) curve(0) 27 }
ansip256r1	{ iso(1) member-body(2) us(840) 10045 curves(3) prime(1) 7 }
ansit283k1	{ iso(1) identified-organization(3) certicom(132) curve(0) 16 }
ansit283r1	{ iso(1) identified-organization(3) certicom(132) curve(0) 17 }
ansip384r1	{ iso(1) identified-organization(3) certicom(132) curve(0) 34 }
ansit409k1	{ iso(1) identified-organization(3) certicom(132) curve(0) 36 }

ansit409r1	{ iso(1) identified-organization(3) certicom(132) curve(0) 37 }
ansip521r1	{ iso(1) identified-organization(3) certicom(132) curve(0) 35 }
ansit571k1	{ iso(1) identified-organization(3) certicom(132) curve(0) 38 }
ansit571r1	{ iso(1) identified-organization(3) certicom(132) curve(0) 39 }

7.1.4 Name Forms

Where required as set forth in Section 3.1.1, the subject and issuer fields of the base certificate shall be populated with an X.500 Distinguished Name. Distinguished names shall be composed of standard attribute types, such as those identified in [RFC3280].

7.1.5 Name Constraints

DHS CAs shall assert name constraints in certificates issued to external CAs and subordinate CAs as appropriate.

7.1.6 Certificate Policy Object Identifier

All certificates issued by DHS CAs shall include a certificate policies extension asserting the OID(s) appropriate to the level of assurance with which it was issued. See Section 1.2 for specific OIDs.

7.1.7 Usage of Policy Constraints Extension

No stipulation.

7.1.8 Policy Qualifiers Syntax & Semantics

DHS CAs shall avoid issuing certificates containing policy qualifiers. If a DHS CA issues certificates containing policy qualifiers, they must be identified in the applicable CPS and are constrained to the policy qualifiers identified in [RFC 3280].

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

Certificates issued by DHS CAs shall not include a critical certificate policies extension.

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

For DHS CAs, CRL extensions shall conform to [FPKI-PROF].

7.3 OCSP Profile

Certificate Status Servers (CSSs) operated under this policy shall sign responses using algorithms designated for CRL signing.

CSSs shall be able to process SHA-1 hashes when included in the CertID field and the keyHash in the responderID field.

7.3.1 Version Number(s)

CSSs operated under this policy shall use OCSP version 1.

7.3.2 OCSP Extensions

Critical OCSP extensions shall not be used.

8.0 COMPLIANCE AUDIT & OTHER ASSESSMENTS

The DHS PKI PA shall have a compliance audit mechanism in place to ensure that the requirements of this DHS CP, any applicable MOAs, and DHS CAs' CPSs are being implemented and enforced.

This specification does not impose a requirement for any particular assessment methodology.

For DHS CAs dedicated to issuing certificates for FIPS 201 Personal Identity Verification Cards, the audit requirement for the Local Registration Authority functions specified in this CP will be met by FISMA audit of the PIV Card Issuing Organization performed in accordance with *NIST Special Publication 800-79 Guidelines for Certification and Accreditation of PIV Card Issuing Organizations*.

8.1 Frequency Of Audit Or Assessments

The DHS Root CA and RA and DHS subordinate CAs and RAs shall be subject to a periodic compliance audit at least once per year for High, Medium Hardware, Medium, and Card Authentication Assurance, and at least once every two years for Basic Assurance. Where a status server is specified in certificates issued by a CA, the status server shall be subject to the same periodic compliance audit requirements as the corresponding CA. For example, if an OCSP server is specified in the authority information access extension in certificates issued by a CA, that server must be reviewed as part of that CA's compliance audit.

For DHS CAs operated by federal agencies and DHS CAs operated under federal contract, alternative reviews may be substituted for full compliance audits under exceptional circumstances. The conditions that permit an alternative review are as follows:

(1) If no changes to policies, procedures, or operations have occurred during the previous year, an assertion to that effect, signed by the cognizant executive (CIO or equivalent), is acceptable in lieu of a full compliance audit.

(2) If no significant changes to policies, procedures, or operations have occurred during the previous year, a delta compliance audit is acceptable in lieu of a full compliance audit.

(3) However, a full compliance audit (see section 8.4) must be completed every third year regardless.

Practice Note: Examples of significant changes include but are not limited to: (i) installation of a new or upgraded operating system, middleware component, or application; (ii) modifications to CA and or RA operating procedures; (iii) installation of a new or upgraded hardware platform or firmware component; and (iv) modifications to the certificate policy. This is consistent with the requirements that trigger a full C&A in NIST SP 800-37.

There is no audit requirement for CAs and RAs operating at the Rudimentary and Internal Basic level of assurance.

The DHS PKI PA has the right to require periodic and aperiodic compliance audits or inspections of DHS CA, RA or CSS operations to validate that the subordinate entities are operating in accordance with the security practices and procedures described in their respective CPS. The DHS PKI PA shall state the reason for any aperiodic compliance audit.

8.2 Identity & Qualifications Of Assessor

The auditor must demonstrate competence in the field of compliance audits. At the time of the audit, the DHS PKI compliance auditor must be thoroughly familiar with requirements which the Federal PKI Policy Authority imposes on the issuance and management of DHS CA certificates. Likewise, the compliance auditor must be thoroughly familiar with the requirements which DHS imposes on the issuance and management of DHS CA certificates. The compliance auditor must perform such compliance audits as a regular ongoing business activity.

The auditor should be a Certified Information System Auditor (CISA), IT security specialist, and a PKI subject matter specialist who can offer input regarding acceptable risks, mitigation strategies, and industry best practices. The FPKI OA shall identify and the compliance auditor for the DHS PKI.

The DHS PKI PA shall determine whether a compliance auditor meets this requirement.

8.3 Assessor's Relationship To Assessed Entity

For the DHS PKI, the compliance auditor either shall be a private firm, that is independent from the entity being audited, or it shall be sufficiently organizationally separated from that entity to provide an unbiased, independent evaluation. An example of the latter situation may be an Agency inspector general.

The DHS PKI PA shall determine whether a compliance auditor meets this requirement.

For DHS audit reports submitted to the Federal PKI Policy Authority to obtain or maintain cross certifications with the FBCA, the Federal PKI Policy Authority shall determine whether the compliance auditor meets this requirement.

8.4 Topics Covered By Assessment

The purpose of a compliance audit of a DHS CA shall be to verify that the CA is complying with the requirements of the DHS CP, operating in accordance with the governing CPS, as well as complying with any MOAs between the DHS CA and any external entity PKI.

A full compliance audit for the DHS PKI covers all aspects within the scope identified above.

Where permitted by section 8.1, a DHS CA may perform a delta compliance audit in lieu of the full compliance audit. A delta compliance audit covers all changes to policies, procedures, or operations that have occurred during the previous year. The following topics must be addressed in a delta compliance audit even if no changes have occurred since the last full compliance audit:

- Personnel controls;
- Separation of Duties;
- Audit review frequency and scope;
- Types of events recorded in physical and electronic audit logs;
- Protection of physical and electronic audit data;
- Physical security controls; and
- Backup and Archive generation and storage.

8.5 Actions Taken As A Result Of Deficiency

When the DHS PKI compliance auditor finds a discrepancy between how a DHS CA is designed or is being operated or maintained, and the requirements of the DHS CP, any applicable MOAs, or the applicable CPS, the following actions shall be performed:

- The compliance auditor shall document the discrepancy;
- The compliance auditor shall promptly notify the DHS PKI OA and DHS PKI PA;
- The DHS PKI PA shall determine what further notifications or actions are necessary to meet the requirements of the DHS CP, CPS, and any relevant MOA provisions. The DHS PKI PA shall proceed to make such notifications and take such actions without delay.
- The DHS PKI PA shall determine an appropriate remedy that includes a time for completion. Remedies may include permanent or temporary CA, CSS, 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.

8.6 Communication Of Results

An annual Audit Compliance Report letter shall be provided by the DH S PKI PA to the Federal PKI Policy Authority. The report shall identify the versions of the CP and CPS(s) used in the assessment. Additionally, where necessary, the results shall be communicated as set forth in Section 8.5 above.

9.0 OTHER BUSINESS & LEGAL MATTERS

9.1 Fees

The DHS PKI Policy Authority reserves the right to charge a fee for any or all services provided.

9.1.1 Certificate Issuance/Renewal Fees

No Stipulation.

9.1.2 Certificate Access Fees

No Stipulation.

9.1.3 Revocation or Status Information Access Fee

No Stipulation.

9.1.4 Fees for other Services

No Stipulation.

9.1.5 Refund Policy

No Stipulation.

9.2 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.

9.2.1 Insurance Coverage

No stipulation.

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance/Warranty Coverage for End-Entities

No stipulation.

9.3 Confidentiality Of Business Information

DHS PKI information not requiring protection shall be made publicly available. MOAs between the DHS PKI PA and external entities shall determine access by either party to the other party’s information.

9.3.1 Scope of Confidential Information

The following information shall also be considered confidential and may not be disclosed except as detailed in Sections 9.3.3 through 2.8.7:

- Audit trail records created and retained by the PKI;
- Security measures of the PKI and its operation;
- Disaster recovery plans;
- Information concerning the events leading up to, and the investigation of a revocation; and
- Information protected by the Privacy Act of 1974.

9.3.2 Information Not Within the Scope of Confidential Information

To promote the interoperation and widespread utility of PKI services, information included in certificates or in the PKI repository are not considered confidential.

9.3.3 Responsibility to Protect Confidential Information

Sensitive information must be stored securely, and may be released only in accordance with other stipulations in Section 9.4.

9.4 Privacy Of Personal Information

9.4.1 Privacy Plan

The DHS PKI OA shall conduct a Privacy Impact Assessment. If deemed necessary, the DHS PKI OA shall have a Privacy Plan to protect personally identifying information from unauthorized disclosure. The DHS PKI PA shall approve the Privacy Plan.

9.4.2 Information Treated as Private

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.

9.4.3 Information Not Deemed Private

Information included in DHS CA certificates and CRLs are not subject to protections outlined in Section 9.4.2. However, certificates that contain the FASC-N in the subject alternative name extension, such as PIV Authentication Certificates, shall not be distributed via public repositories (e.g., via LDAP or HTTP).

9.4.4 Responsibility to Protect Private Information

Sensitive information must be stored securely, and may be released only in accordance with other stipulations in Section 9.4.

9.4.5 Notice and Consent to use Private Information

The DHS PKI OA is not required to provide any notice or obtain the consent of the Subscriber or Entity personnel in order to release private information in accordance with the stipulations of Section 9.4.

9.4.6 Disclosure Pursuant to Judicial/Administrative Process

The DHS PKI Operational Authority shall not disclose private information to any third party unless authorized by this Policy, required by law, government rule or regulation, or order of a court of competent jurisdiction. Any request for release of information shall be processed according to 41 CFR 105-60.605.

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 Operational Authority or DHS CAs are not obligated to inform the Subscriber of such release.

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.

9.4.7 Other Information Disclosure Circumstances

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.

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

9.5 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.

The DHS PKI OA and DHS CAs will not knowingly violate intellectual property rights held by others.

9.6 Representations & Warranties

The obligations described below pertain to all DHS CAs (and, by implication, the DHS PKI OA).

9.6.1 CA Representations and Warranties

DHS CA certificates are issued and revoked at the sole discretion of the DHS PKI PA.

When a DHS CA issues a cross-certificate, it does so for the convenience of the U.S. Department of Homeland Security. Any review by the DHS PKI PA of a non-DHS entity's certificate policy is for the use of the DHS PKI PA in determining whether or not interoperability is possible, and if possible, to what extent the non-DHS entity's certificate policy maps to the DHS certificate policy.

A non-DHS entity must determine whether that entity's certificate policy meets its legal and policy requirements. Review of a non-DHS entity's certificate policy by the DHS PKI PA is not a substitute for due care and mapping of certificate policies by the non-DHS entity.

Each DHS CA shall be operated in compliance with this CP and the CPS for that CA.

9.6.2 RA Representations and Warranties

RAs for each DHS CA shall perform their functions in compliance with this CP and the CPS for that CA. If the CPS allows the use of LRAs or TAs, they shall perform their functions in compliance with this CP and the CPS for that CA.

9.6.3 Subscriber Representations and Warranties

For Medium, Card Authentication, Medium Hardware, and High Assurance levels, a Subscriber, or an authorized Sponsor representing a non-human Subscriber, shall be required to sign a document containing the requirements the Subscriber shall meet respecting protection of the private key and use of the certificate before being issued the certificate. For the Internal Basic and Basic Assurance levels, the Subscriber, or an authorized Sponsor representing a non-human Subscriber, shall be required to acknowledge his or her obligations respecting protection of the private key and use of the certificate before being issued the certificate.

Subscribers of DHS CAs, or authorized Sponsors representing the non-human Subscribers, at Internal Basic, Basic, Medium, Card Authentication, Medium Hardware and High Assurance levels shall agree to the following:

- Subscribers and Sponsors shall accurately represent themselves in all communications with the PKI authorities;
- Subscribers shall protect their private keys at all times, in accordance with this policy, as stipulated in their certificate acceptance agreements (DHS Subscriber Agreement);
- Subscribers shall protect the private keys of the non-human Subscriber they represent at all times, in accordance with this policy, as stipulated in their certificate acceptance agreements (DHS Sponsor Agreement);
- Subscribers shall promptly notify the appropriate CA upon suspicion of loss or compromise of their private keys. Such notification shall be made directly or indirectly through mechanisms consistent with the issuing CA's CPS;
- Sponsors shall promptly notify the appropriate CA upon suspicion of loss or compromise of the private keys of the non-human Subscriber they represent. Such notification shall be made directly or indirectly through mechanisms consistent with the issuing CA's CPS;

- Subscribers shall abide by all the terms, conditions, and restrictions levied on the use of their private keys and certificates; and
- Sponsors shall abide by all the terms, conditions, and restrictions levied on the use of the private keys and certificates of the non-human Subscriber they represent.

9.6.4 Relying Parties Representations and Warranties

None.

9.6.5 Representations and Warranties of other Participants

None.

9.7 Disclaimers Of Warranties

No stipulation.

9.8 Limitations of 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.

9.9 Indemnities

No stipulation.

9.10 Term & Termination

9.10.1 Term

This CP becomes effective when approved by the DHS PKI Policy Authority. New DHS CAs that initiate operations after this CP is approved, shall be operated in compliance with this CP from their inception.

Existing DHS CAs, operating under the previous approved version of this DHS CP, shall implement the revised practices required to comply with the policy changes implemented by this DHS CP as soon as practical, but no later than May 31, 2007. The DHS PKI Policy Authority may require existing DHS CAs to comply with specific policy changes prior to May 31, 2007.

This CP has no specified term.

9.10.2 Termination

Termination of this CP is at the discretion of the DHS PKI Policy Authority.

9.10.3 Effect of Termination and Survival

None.

9.11 Individual Notices & Communications With Participants

None.

9.12 Amendments

9.12.1 Procedure for Amendment

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 CAs, Subscribers and Relying Parties.

9.12.2 Notification Mechanism and Period

This CP and any subsequent changes shall be made publicly available.

9.12.3 Circumstances Under Which OID Must Be Changed

OIDs will be changed if the DHS PKI PA determines that a change in the CP reduces the level of assurance provided.

9.13 Dispute Resolution Provisions

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.

Any dispute arising with respect to this policy or certificates issued under this policy shall be resolved by the Parties.

9.14 Governing Law

The construction, validity, performance and effect of certificates issued under this CP for all purposes shall be governed by United States Federal law (statute, case law or regulation).

Where an inter-governmental dispute occurs, resolution will be according to the terms of the MOA.

9.15 Compliance With Applicable Law

No stipulation.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

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 9.12.

9.16.4 Enforcement (Attorney Fees/Waiver of Rights)

No stipulation.

9.16.5 Force Majeure

No stipulation.

9.17 Other Provisions

No stipulation.

10.0 BIBLIOGRAPHY

The following documents were used in part to develop this CP:

[ABADSG] *Digital Signature Guidelines,* American Bar Association, August 1, 1996, http://www.abanet.org/scitech/ec/isc

[ABAPAG] *PKI Assessment Guidelines,* American Bar Association, June 18, 2001, http://www.abanet.org/scitech/ec/isc

[CIMC] *Certificate Issuing and Management Components Family of Protection Profiles, Version 1.0, October 31, 2001*

[CPFCP] *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework,* Version 2.1, January 12, 2006, http://www.cio.gov/fpkipa

[DOSCP] *X.509 Certificate Policy for the United States Department of Defense*, Version 9.0, February 9, 2005

[FBCACP] *Draft X.509 Certificate Policy for the Federal Bridge Certification Authority (FBCA),* Version 3647 – 0.2, December 23, 2005

[FIPS 140-2] Federal Information Processing Standards (FIPS) Publication (Pub) 140-2: *Security Requirements for Cryptographic Modules,* May 2001, http://csrc.nist.gov/publications/fips

[FIPS 186-2] Federal Information Processing Standards (FIPS) 186-2: *Digital Signature Standard (DSS),* January 2000, http://csrc.nist.gov/publications/fips

[FIPS 201-1] Federal Information Processing Standards (FIPS) 201-1: *Personal Identity Verification (PIV) of Federal Employees and Contractors*, March 2006, http://csrc.nist.gov/publications/fips

[FOIACT] 5 U.S.C. 552, Freedom of Information Act. Http://www4.law.cornell.edu/uscode/5/552.html

[FPKI-PROF] *Federal Public Key Infrastructure (PKI) X.509 Certificate and CRL Extensions Profile*, October 12, 2005, http://www.cio.gov/fpkipa

[IC] *X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Providers (SSP) Program* , February 6, 2006, http://www.cio.gov/ficc

[NARARMP] *Records Management Guidance for PKI-Unique Administrative Records*, March 14, 2002, http://www.archives.gov/records-mgmt/policy/final-pki-guidance

[RFC 3280] Request for Comments (RFC) 3280: *Internet X.509 Public Key Infrastructure Certificate and CRL Profile*, April 2002, http://www.ietf.org/rfc

[RFC 3647] Request for Comments (RFC) 3647: *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*, November 2003, http://www.ietf.org/rfc

[SP800-78] NIST Special Publication 800-78: *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*, April 2005, http://www.csrc.nist.gov/publications/nistpubs

[SP800-79] NIST Special Publication 800-79: *Guidelines for Certification and Accrediatation of PIV Card Issuing Organizations*, July 2005, http://www.csrc.nist.gov/publications/nistpubs

11.0 ACRONYMS & ABBREVIATIONS

AES	Advanced Encryption Standard
CA	Certification Authority
CAKC	CA Key Custodian
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSS	Certificate Status Service
CSOR	Computer Security Object Registry
DES	Data Encryption Standard
DHS	Department of Homeland Security
DN	Distinguished Name
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
ECDSA	Elliptic Curve Digital Signature Algorithm
FASC-N	Federal Agency Smart Credential Number
FBCA	Federal Bridge Certification Authority
FIPS	Federal Information Processing Standard
FISMA	Federal Information System Management Act
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 (*see also* Glossary definition)
MOU	Memorandum of Understanding
NIST	National Institute of Standards and Technology
OA	Operational Authority
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PA	Policy Authority
PCA	Principal Certification Authority
PIN	Personal Identification Number
PIV	Personal Identity Verification
PIVCIO	Personal Identity Verification Card Issuing Organization
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509 (IETF Working Group)
PPCO	PKI Policy Compliance Officer
PSM	PKI Service Manager
PSS	Probabilistic Signature Scheme
Pub	Publication
RA	Registration Authority
RFC	Request For Comments
RSA	Rivest-Shamir-Adleman (encryption algorithm)
SBU	Sensitive-But-Unclassified
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
TLS	Transport Layer Security
URL	Uniform Resource Locator
U.S.C.	United States Code
WWW	World Wide Web

12.0 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.

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.

CA Key Custodian (CAKC)

CA Key Custodians are government employees who control access to CA keying materials containing CA signing keys.

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 Service (CSS)

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.

Content Signer

An entity that digitally signs the Cardholder Unique Identifier on the Personal Identity Verification smart card (see [FIPS 201]).

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.

FPKI Operational Authority

The Federal Public Key Infrastructure 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.

Personal Identity Verification Card Issuing Organization (PIVCIO)
The DHS organization responsible for issuing Personal Identity Verification (PIV) Cards that comply with FIPS 201 to DHS employees and contractor employees, and for life cycle management of the cards and their content.

PKI Policy Compliance Officer (PPCO)
The PKI Policy 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.

PKI Service Manager
The PKI Service Manager works for the DHS PKI Operational Authority and is responsible for managing PKI operations.

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.

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.