U.S. Department of Energy

Public Key Infrastructure

X.509 Certificate Policy

United States Department of Energy

Version 2.0

July 25, 2003

DRAFT

Revision History

Date	Version	Description	Author
5/31/03	1.0	Import information from CP-1S Draft 1e – August 31, 1999 and adapt meet current RFC 2527 format, Bridge model CP, and FBCA requirements.	Booz Allen Hamilton
6/12/03	1.1	Changes approved by the DOE PKITWG during workshop	PKI Working Group, Booz Allen Hamilton
6/16/03	1.2	Edited Changes as approved by DOE PKI TWG after workshop	Booz Allen Hamilton
6/20/03	1.3	More changes made, approved by DOE PKI TWG.	Booz Allen Hamilton
7/15/03	1.8	Final draft edits. Stage I.	Booz Allen Hamilton
7/25/03	2.0	Final draft edits. Stage II	Booz Allen Hamilton
8/4/03	2.1	Final draft edits. Stage III	Booz Allen Hamilton
8/5/03	2.2	Final draft edits. Stage IV	Booz Allen Hamilton

Signature Page

Chief Information Officer Department of Energy	DATE
Associate CIO for CyberSecurity Department of Energy	DATE
General Counsel Department of Energy	DATE

TABLE OF CONTENTS

Page

TABLES

1 INTRODUCTION

The DOE PKI is a general-purpose utility that supports or provides services to other applications. It is an application and process enabler that adds capabilities to a digital work environment to establish uniform methods of creating trust and reliance attributes otherwise missing from that environment. It provides certificate services and supports common identity and policy-based access functions within DOE networks and includes the Certification Authorities (CAs) at various DOE sites.

The DOE PKI will support or provide the following to DOE applications and security services:

- ***Authentication*** is the assurance that the information originator and consumer may both be identified uniquely. In the context of electronic messaging systems, it supports additional functionality so that both parties know where the information is coming from and where it is going.
- ***Confidentiality***, or privacy, is the assurance that information and data will be protected from unauthorized access.
- ***Data integrity*** is the assurance that data has not been accidentally or deliberately altered.
- ***Non-Repudiation*** provides proof of the integrity and origin of data that can be verified by a third party. Non-repudiation services may provide important legal evidence in the event of a dispute.

The operation of the DOE PKI and its components involves the following security management services:

- Key Generation/Storage/Recovery,
- Certificate Generation, Update, Renewal, Re-key, and Distribution,
- Certificate Revocation List (CRL) Generation and Distribution,
- Directory management of certificate related items,
- Certificate token initialization/programming/management, and;
- Privilege and authorization management.
- Defining requirements on PKI activities, including the following, ensures the security of these services:
- End Entity authentication verification,
- Control of computer and cryptographic systems,
- Operation of computer and cryptographic systems,
- Usage of keys and public key certificates by End Entities and relying parties,
- Definition of rules to limit liability and to provide a high degree of certainty that the stipulations of this policy are being met, and;

- System Management Functions (e.g. security audit, configuration management, certificate tracking, archive).

The reliability of the overall security solution is the result of the trustworthy operation of the DOE PKI (commensurate with the medium assurance level), including equipment, facilities, personnel, and procedures. The Certificate Policy (CP) is a published set of rules that govern the operation of the PKI, and may be used by a certificate user to measure the trustworthiness of a certificate, and the binding therein, for a particular application.

All DOE Certificate Authorities (CAs) will be supported by a single policy for the use of digital signatures and encryption applications. The scope of this CP may be expanded to cover multiple policies when the need for multiple assurance levels for various applications become apparent. This policy will provide recommended baseline security requirements for the use and operation of CAs, Registration Authorities (RAs), and other PKI Components within the DOE PKI. This document defines the policy under which the DOE PKI will be established and operate.

The Department of Energy and its Operating Units are eligible to participate in the DOE PKI.

1.1 Overview

1.1.1 Certificate Policy (CP)

This is a Certificate Policy (CP) for issuance, management, and use of public key certificates and associated cryptographic technology used for authentication, confidentiality, data integrity, and non-repudiation security services in DOE unclassified information processing communities. This Policy also includes operation of peer Certification Authorities (CAs) that issue and manage these certificates.

This CP states the roles and obligations of CAs and other entities issuing, managing, and using certificates and related cryptographic materials. It sets forth requirements for authentication of entities, operation of CA software and hardware, and cross-certifications with other CAs, and other essential elements of certificate issuance, management, and use.

This CP is termed a medium assurance level policy with respect to measures specified for assuring trust, authentication, key lengths, physical and computer security protections, etc and is intended to be consistent with the FBCA medium assurance policy.

This CP establishes standards that allow relying parties to use public key certificates (issued and managed by a CA) with assurance that the certificates are acceptable for the security services stated above.

A mandatory requirement of this Policy is that each operator of a complying CA publishes and gains approval for a Certification Practice Statement (CPS) that references this Policy by name, and specifies methods and procedures for implementing this Policy. It is recommended that the CPS be developed in accordance with the CPS framework document cited in the References section of this Policy.

1.1.1.1 Important Terminology Used in the DOE CP

It is critical to understanding of this CP that the following terms are defined:

DOE PKI –This term refers to the aggregation of all Certification Authorities (CAs) that assert this policy, and the other PKI components (Registration Authorities, Directories, Certificate Policies and Certificate Practice Statements) that are used to provide digital signature and encryption key certificates to DOE Subscribers. This term will not be abbreviated to avoid confusion.

DOE Principal CA – The Principal CA is the CA that certifies all individual Site CAs (or ***DOE Site CA***s). This CA performs cross-certification with the Federal Bridge CA. The Principal CA does not issue certificates to subscribers.

DOE Site CA – Site CAs are the "operational" CAs that are certified by the Principal CA and issue certificates to individuals in the DOE.

DOE Certification Authorities (DOE CAs) – Refers to both the Principal CA and all Site CAs.

1.1.2 Relationship Between the DOE CP and the DOE CPS

The DOE CP states what assurance can be placed in a certificate issued by the DOE PKI. DOE CPS(s) state how the applicable DOE Site CA establishes that assurance. The links to all non-sensitive DOE PKI documents can be found on the DOE PKI web site, http://pki.doe.gov/.

1.1.3 Interoperation with CAs External to the Department of Energy

The current version of this CP provides for interoperability with the FBCA through cross certification with the DOE Principal CA and interoperability within the DOE PKI infrastructure through the DOE Principal CA architecture and communication with external (non-Federal) parties through cross certification with either the DOE PCA or DOE Site CAs. Such interoperability will be established when directed by the DOE-PMA (DOE Policy Management Authority).

In particular, this document defines the Medium-level CP for CAs within the DOE PKI. CAs external to the DOE may wish to cross-certify with the CA(s) internal to the DOE PKI, for the purpose of issuing certificates to support interoperability, enhanced security communications with internal DOE users. These CAs need to meet or exceed all requirements contained in this policy document.

1.1.4 Interoperation with CAs External to the Federal Government

Interoperability of the PKI with other entities will be established when directed by the DOE-PMA, and may require changes to this CP to address issues associated with liability and other matters.

1.1.5 Scope

The current version of this CP provides for interoperability between the DOE Principal CA, DOE Site CAs, and Federal PKI (FPKI) domains only. This CP applies to medium assurance certificates only. Separate Certificate Policies will be developed in the future if the Department decides to support other assurance levels (so that each level has its own policy).

1.2 Identification

The OID is registered under the id-infosec arc as follows: TBD.

Table 1.4-1 DOE Registered OID

doe-medium	::={ TBD }

1.3 Community and Applicability

Certificates issued under this Policy are intended for use within the DOE unclassified community. The following are roles relevant to the administration and operation of the DOE PKI.

1.3.1 PKI and PKI Related Authorities

1.3.1.1 DOE Policy Management Authority (DOE-PMA)

The DOE-PMA is responsible for the direction and operation of the PKI. Chaired by the Associate Chief Information Officer for Cyber Security, the Authority will be composed as described in the Trusted Roles section in the pertinent DOE CPS. The DOE-PMA is responsible for:

- Approval of the DOE CP,
- Approval of a DOE CPS, a document that assures that the practices of the applicable DOE Site CA comply with this CP,
- Determining the levels of assurance set forth in the DOE CP, and for;
- Ensuring continued conformance with the DOE CP and Concept of Operations (CONOPS).

In the event the DOE Principal CA cross-certifies with another CA, the DOE-PMA will enter into a Memorandum of Agreement (MOA) or similar instrument with an organization setting forth the respective responsibilities and obligations of both parties, and the mappings between the certificate levels of assurance contained in this CP. Thus, the term “MOA” as used in this CP refers to the Memorandum of Agreement cited in this paragraph.

The DOE-PMA is comprised of the Policy Approving Authority (PAA), the Policy Certification Authority (PCA), a representative of each site that is operating a CA, and/or other representatives from sites participating in the DOE PKI. The PMA must operate under the oversight of the PCA and address issues that affect the DOE PKI. Below are further details about the PAA and PCA as specified in the DOE PKI Policy Document:

- Policy Approving Authority. The Chief Information Officer, SO-30, serves as the DOE PAA. The PAA evaluates and approves overall PKI policy and practices and manages the

certificates. The PAA delegates oversight for PKI operation to the PCA and periodically reviews PCA practices for consistency and operational efficiency.

- Policy Certification Authority. The Office of Chief Information Officer, Office of Cyber Security (SO-33), serves as the DOE PCA. The PCA is the chair of the PMA and is responsible for developing and issuing policy, approving CP(s), reviewing CPS(s), and conducting assistance visits for the CAs. The PCA, through the PMA, is also responsible for coordinating distinguished names for the CAs, maintaining a master registration list of all DOE CAs and CP(s), and providing policy object identifiers for all approved CP(s).

1.3.1.2 DOE Legal Authority (DOE-LA)

The DOE-LA is responsible for legal support to the DOE-PMA concerning all matters in the jurisdiction of the DOE-PMA and shall be chaired by the Office of General Counsel.

1.3.1.3 DOE Operational Authority

The DOE Operational Authority is the organization that governs the operation of CAs within the DOE, including issuing CA certificates when directed by the DOE-PMA, posting those certificates and Certificate Revocation Lists (CRLs) into the repository, and ensuring the continued availability of the repository to all users. The DOE Operational Authority shall be chaired by the DOE-PMA.

1.3.1.4 DOE Operational Authority Administrator

The DOE Operational Authority Administrator, appointed by the DOE Operational Authority, is a role who has principal responsibility for overseeing the proper operation of the CA and who is also responsible for the repository. This responsibility shall lie within the Office of the Associate CIO for Cyber Security.

1.3.1.5 DOE Operational Authority Officers

The DOE Operational Authority Officers is a role; the individuals are selected by the DOE Operational Authority and operate the CA and its repository including executing DOE Operational Authority directions to issue CA certificates to CAs or take other action to effect interoperability between the DOE Principal CA and other CAs.

1.3.1.6 DOE Naming Authority (DOE-NA)

The DOE-NA is responsible for the creation of Distinguished Names and other naming conventions in support of PKI and Directory Services. The Office of the Associate CIO for Cyber Security shall chair the DOE-NA. The DOE-NA is described in greater detail in Sections 3.1.1 and 3.1.2 below.

1.3.1.7 DOE PKI

The DOE PKI is the aggregation of entities (e.g. CAs) that are authorized by the DOE-PMA to create, sign, and issue public key certificates to DOE employees, contractors, partners, and other

End Entities as appropriate. As operated, the DOE Site CAs are responsible for all aspects of the issuance and management of a certificate, including –

- Control over the registration process,
- The authentication process,
- The certificate manufacturing process,
- Publication of certificates,
- Revocation of certificates,
- Re-key of DOE Site CA signing material, and;
- Ensuring that all aspects of the DOE PKI services and DOE PKI operations and infrastructure related to certificates issued under this CP are performed in accordance with the requirements, representations, and warranties of this CP.

1.3.1.8 DOE Site Registration Authority Administrator (DOE-SRAA)

The DOE-SRAA is the entity that collects and verifies each End Entity's identity and information that is to be entered into the End Entity's public key certificate. The DOE-SRAA performs registration and identity proofing on behalf of a DOE Site CA, and performs its function in accordance with a DOE CPS approved by the DOE-PMA. The DOE-SRAA uses the DOE Site Registration Authority (DOE-RA) equipment to perform the registration functions. The requirements for RAAs are set forth in the sections below.

1.3.2 Related Entities

CAs operating under this policy will require the services of other security, community, and application entities, such as auditors and attribute entities. The DOE CPS would identify the roles responsible for providing such services, and the mechanisms used to support these services.

1.3.3 End Entities and Relying Parties

1.3.3.1 End Entities

An End Entity is the person whose name appears as the subject in a certificate. The End Entity asserts that he or she uses the key and certificate in accordance with the certificate policy asserted in the certificate, and does not issue certificates. End Entities include all organizational personnel and possibly hardware devices or software modules such as firewalls and routers when needed for infrastructure protection.

1.3.3.2 Relying Parties

A relying party is the entity that relies on the validity of the binding of the End Entity's name to a public key. The relying party is responsible for deciding whether or how to check the validity of the certificate by checking the appropriate certificate status information. A relying party may

use information in the certificate (such as CP identifiers) to determine the suitability of the certificate for a particular use.

1.3.4 Applicability

The sensitivity of the information processed or protected using certificates issued by DOE CAs will vary significantly. Organizations 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 organization for each application and is not controlled by this CP. To provide sufficient granularity, this CP specifies security requirements for the Medium Assurance Level as generally defined by the FPKI Steering Committee. This policy is applicable only for applications involving unclassified information, which can include sensitive but unclassified data protected pursuant to federal statues and regulations.

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

The Medium Assurance Level provides an assurance of confidentiality, information integrity, authentication and non-repudiation to a broad array of business transactions and exchanges. This level is relevant to environments where risks and consequences of data compromise are moderate and can cause significant damage to an organization or its trading partners. 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.

It is suitable for transactions requiring authentication and is sufficient for high volume and moderate-to-high value transactions requiring confidentiality.

1.3.4.1 Factors in determining usage

The Relying Party must first determine the level of assurance required for an application, and then select the certificate appropriate for meeting the needs of that application. This will be determined by evaluating various risk factors including the value of the information, the threat environment, and the existing protection of the information environment. These determinations are made by the Relying Party and are not controlled by the DOE-PMA or the DOE-OA. Nonetheless, this CP contains some helpful guidance, set forth below, which Relying Parties may consider in making their decisions. Further, 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 an Budget (OMB) 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 NIST Special Publication 800-25 covering the technical elements of using digital signatures, and electronic record retention guidance such as that provided by the National Archives and Records Administration at http://www.nara.gov/policy/gpea and http://www.cio.gov/docs/NARA_gpea).

1.4 Contact Details

1.4.1 Specification Administration Organization

The DOE-PMA is responsible for all aspects of this CP.

1.4.2 Contact Person

Questions regarding this CP shall be directed to the DOE-PMA via the Director of Engineering and Assessment in the Office of Cyber Security at the Department of Energy, 19901 Germantown Road, Germantown MD 20874.

1.4.3 Person determining Certification Practice Statement suitability for the policy

Each DOE Site that is operating a CA that asserts to this CP, will document its operating practices in a CPS. All CPS(s) will be reviewed by the DOE Operating Authority and approved for suitability for this CP by the DOE-PMA via the Directory of Engineering and Assessment in the Office of Cyber Security at the Department of Energy who resides at 19901 Germantown Road, Germantown Road, Germantown MD 20874.

2 GENERAL PROVISIONS

2.1 Obligations

The obligations described below pertain to the DOE PKI.

2.1.1 DOE PKI Obligations

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

- Providing to the DOE-PMA a CPS, as well as any subsequent changes, for conformance assessment,
- Conforming to the stipulations of the approved CPS,
- Ensuring that registration information is accepted only from SRAAs who understand and are obligated to comply with this policy,
- Including only valid and appropriate information in the certificate, and maintaining evidence that due diligence was exercised in validating the information contained in the certificate,
- Ensuring that obligations are imposed on End Entities in accordance with section 2.1.5, and that End Entities are informed of the consequences of not complying with those obligations,
- Revoking the certificates of End Entities found to have acted in a manner counter to those obligations,
- Ensuring that obligations are imposed on non-U.S. Government End Entities in accordance with the provisions of section 2.1.8, and;
- Operating the services of an online repository that satisfies the obligations under section 2.1.7, and informing the repository service provider of those obligations if applicable.

The following are additional DOE Certification Authority obligations:

- Accuracy of representations – Each DOE Certification Authority is obligated to all who reasonably rely on the information contained in a certificate, to warrant that it has issued the certificate to the named End Entity and that End Entity has accepted the certificate.
- Notification of certificate issuance – Each DOE Certification Authority is obligated to ensure that the End Entity who is the subject of a certificate and others who reasonably rely on that certificate are notified of the certificate issuance. Publication in the directory shall constitute notification.
- Notification of revocation or suspension of a certificate – Each DOE Certification Authority is obligated to ensure that the End Entity who is the subject of a certificate and others who reasonably rely on that certificate are notified of the certificate revocation or

suspension in accordance with sections 4.4.1 through 4.4.2 of this policy. Publication of CRLs and ARLs in the directory shall constitute notification.

2.1.2 DOE-RA and DOE-SRAA Obligations

A DOE-RA is the software and hardware that communicates with a DOE CA to request certificates on behalf of End Entities. The DOE Site Registration Authority Administrator (DOE-SRAA) performs registration functions such as identity proofing and delivery of activation data as described in this policy and in the applicable DOE CPS and shall comply with the stipulations of this policy, and comply with the applicable DOE CPS approved by the DOE-PMA for use with this policy. A DOE-SRAA who is found to have acted in a manner inconsistent with these obligations is subject to revocation of responsibilities and authorities.

The division of PKI duties between each DOE Site CA and RA may vary as provided in the applicable Site CA CPS. For example, the site RA may collect information for a DOE Site CA only, or it may build the certificate for the CA to sign. Only those who understand the DOE CP requirements, and must agree to abide by them must perform DOE-SRAA functions that result in certificate generation, management, and revocation. Security requirements of DOE Site CA's are likewise imposed on any RAAs to the extent that the RAAs are responsible for the information collected.

The following are additional DOE-RA and DOE-SRAA obligations:

- Accuracy of representations — the DOE-SRAA is obligated to accurately represent the information it prepares for a DOE Site CA, to process requests and responses timely and in a manner commensurate with the medium assurance level,
- Maintain certificate application information — the DOE-SRAA is obligated to keep supporting evidence for any certificate request made to a DOE Site CA (e.g., certificate request forms) This is required for compliance with the applicable digital signature, trust verification, and trust path records management requirements prescribed by the National Archives and Records Administration's (NARA) "Records Management Guidance for Agencies Implementing Electronic Signature Technologies" bulletin; and,
- Assist End Entities with registration in the DOE PKI — the DOE-SRAA will be responsible for delivery of activation data to End Entities.

A DOE-SRAA who is authorized to assume other DOE PKI functions may have obligations commensurate with a CAA role; this situation will be described on a case-by-case basis.

2.1.3 Subscriber Sponsor

The sponsor shall be a person or organization with which the subscriber is affiliated (e.g., as an employee, user of service, customer, etc.). The sponsor shall certify that the subscriber has a recognized relationship with the sponsoring organization and has a valid need and purpose for public key certificates issued by the CA. The requirements for sponsoring relationships shall be

specified in the applicable CPS. The sponsor may also certify a group of individuals, in which case each member of the group is considered to be sponsored by the certifying sponsor.

2.1.3.1 Sponsor Representations

By sponsoring an End Entity, the Sponsor certifies that at the time of the Sponsor's approval of the End Entity, and throughout the operational period of the certificate unless the Sponsor notifies the issuing CA or RA otherwise:

- The End Entity has a valid affiliation with the Sponsor (as an employee, user of service, customer, or other relationship documented in the subscription application provided to the CA),
- All representations made by the Sponsor to the CA or RA regarding End Entity information to be used for the issuance of certificates are true, and
- The End Entity has a valid need and purpose for public key certificates issued by the CA.

2.1.3.1.1 Notification of Termination of Sponsoring Relationship

The Sponsor or Sponsor's authorized agent shall notify the CA or RA promptly upon termination of the sponsoring relationship with the End Entity, or termination of the End Entity's valid need for the certificates issued pursuant to that relationship.

2.1.4 Component Sponsors

Some computing and communications components (routers, firewalls, etc.) will be named as certificate subjects. In such cases, the component must have a human Sponsor that has been issued a digital certificate by the DOE CA. The Component Sponsor is responsible for providing the following registration information:

- Equipment identification,
- Equipment name that conforms to the DOE-NA naming convention for such End Entities,
- Equipment public keys,
- Equipment authorizations and attributes (if any are to be included in the certificate),
- Contact information to enable the DOE-CAA or DOE-RAA to communicate with the sponsor when required, and;
- Any other information required by protocols used (such as CEP – the Certificate Enrollment Protocol).

2.1.5 End Entity Obligations

The following are the End Entity obligations:

- Accuracy of representations in certificate applications — End Entities are obligated to accurately represent themselves in all communications with the PKI authorities and other End Entities,
- Protection of End Entity private key — End Entities are obligated to protect their private keys at all times, in accordance with this policy, as stipulated in their certificate acceptance agreements, and local procedures,
- Notification to the Operational Authority upon private key compromise — End Entities are obligated to notify, as soon as practicable, the DOE Operational Authority that issued their certificates of suspicion that their private keys are compromised or lost. Such notification shall be made directly, or indirectly through mechanisms consistent with the DOE CPS or as directed by the End Entity agreement, and;
- Proper use of certificate — End Entities are obligated to abide by all the terms, conditions, and restrictions levied upon the use of their private keys and certificates. Certificates provided by the DOE PKI may only be used for transactions related to government business.

An End Entity that is found to have acted in a manner counter to these obligations will have its certificate revoked, and will have no claim against the DOE PKI in the event of a dispute.

2.1.6 Relying Party Obligations

It is the obligation of the Relying Party to decide whether or not to place trust in the DOE Principal CA and to perform its own certificate path validation leading up to the DOE Principal CA.

2.1.7 Repository Obligations

DOE PKI implementations may use a variety of mechanisms for repository services, including an X.500 Directory Server System, or an LDAP Directory Server. Implementations that do not supply their own repository functions may request service from a DOE Directory Server.

The repository has the obligation to publish certificates and revocation information in a timely manner, upon receipt from a DOE Site CA.

2.1.8 Certificate Issuance to Non-Government Parties

DOE Site CAs may issue certificates to parties other than officers, employees and prime contractors of the Department of Energy, such as subcontractors and commercial vendors, for the convenience of the Department and without fee, when those parties have a bona fide need to possess a certificate issued by the DOE PKI as established by the DOE-PMA. In such a case, a Memorandum of Agreement or similar instrument will be executed, and will contain whatever provisions are determined appropriate by the DOE-PMA. Such a Memorandum of Agreement may be included as amendment or codicil to a Master Agreement through which a Government Contractor agrees to bind itself, all of its employees on the contract for which it requests certificates, and any sub-contractors subsumed under the Master Contract. This removes the

necessity for a separate Memorandum of Agreement (MOA) for each employee of a contractor or subcontractor. The Subscriber Agreement will bind the Subscriber to the MOA. Any Government Contractor for whom a certificate is requested must have the application approved by a Federal Sponsor whom the contractor supports. Such provisions are likely to address the issues delineated below.

2.2 Liability

The DOE PKI warrants only that their procedures are implemented in accordance with their published CP, and that any certificates issued that assert a policy OID defined in this document were issued in accordance with the stipulations of this policy for that level of assurance. DOE-SRAAs warrant that they perform their duties in accordance with applicable sections of this policy, and any CPS(s) or addendums to which they are subject. The terms and provisions of this DOE CP shall be interpreted under and governed by applicable Federal law. The United States Government disclaims any liability, pursuant to section 2.2.1, Damages Covered and Disclaimers, of this DOE CP.

2.2.1 Damages Covered and Disclaimers

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

2.3 Financial Responsibility

Organizations that are acting as relying parties shall determine the financial limits, if any, they wish to impose for certificates used to consummate any financial transaction. Acceptance of Medium Assurance Level certificates is entirely at the discretion of the organization acting as the relying party. Other factors that may influence the relying party's acceptance, in addition to the certificate assurance level, are the likelihood of fraud, other procedural controls in place, organizational-specific policy, or statutorily imposed constraints.

2.3.1 Indemnification by Relying Parties and End Entities

Agents of the DOE PKI assume no financial responsibility.

2.3.2 Fiduciary Relationships

Issuance of certificates in accordance with this certificate policy does not make the DOE PKI, or any DOE-RA or DOE-SRAA, an agent, fiduciary, trustee, or other representative of End Entities or Relying Parties.

2.3.3 Governing Law

The laws of the United States of America shall govern this CP.

2.3.4 Administrative Processes

Administrative processes pertaining to this CP shall be determined by the DOE-PMA pursuant to the agreement between it and the DOE PKI for the operation of all DOE CAs that assert this policy.

2.4 Interpretation and Enforcement

2.4.1 Severability of Provisions, Survival, Merger, and Notice

Should it be determined that one section of this CP is incorrect or invalid, the other sections shall remain in effect until the policy is updated. The process for updating this CP is set forth in section 8.

2.4.2 Dispute Resolution Procedures

The DOE-PMA shall resolve any disputes associated with the use of the DOE certificates issued by the DOE Principal CA or DOE Site CAs.

2.5 Fees

Fees, if any, for government-provided DOE PKI services shall be determined by the DOE-PMA.

2.6 Publication and Repository

2.6.1 Publication of DOE Site CA Information

DOE Site CA's shall provide an on-line repository that is available to End Entities and relying parties and that contains:

- Issued certificates that assert this CP,
- The most recent CRL,
- The DOE Principal CA's certificate for its certificate signing key, and;
- A copy of this Policy, including any waivers granted to the DOE PKI by the DOE-PMA.

2.6.2 Frequency of Publication

Certificates are published as specified in section 2.6. Certificate revocation information is published as specified in section 4.4.1. All information to be published in the repository shall be published promptly after such information becomes available to the DOE Principal CA or peer DOE Site CAs. DOE Site CAs shall specify in their CPS time limits within which it will publish various types of information.

2.6.3 Access Controls

The DOE PKI shall protect any repository information not intended for public dissemination or modification. Public keys and CRLs in the DOE Border PKI directory shall be publicly available through the Internet from the public side of the DOE network. Information in internal directories or repositories shall be accessible as determined by the PMA. The DOE CPS shall detail what information in the repository shall be exempt from automatic availability and to whom, and under which conditions; the restricted information may be made available. Confidentiality matters are addressed in section 2.8 of this Policy.

2.6.4 Repositories

The location of publication will be appropriate to the certificate using community, and in accordance with the local security requirements, see section 2.1.7 for repository obligations. This includes information about certificate owners and agency policies in addition to the directories containing the certificates and CRLs. To facilitate the widest use of certificates, DOE PKI may use an X.500 Directory System in addition to other repositories as deemed appropriate.

2.7 Compliance Audit

DOE CAs will undergo compliance audits to ensure that the requirements of this CP, their respective CPS(s) and the provision of the MOA are being implemented and enforced.

2.7.1 Frequency of Entity Compliance Audit

Each DOE PKI and DOE-RAs shall be subject to a periodic compliance audit that is no less frequent than once per year. Each DOE PKI shall reserve the right to require periodic inspections and audits of any facility that houses a CA within its domain to validate that the CA is operating in accordance with the security practices and procedures laid out in its CPS.

The DOE-PMA reserves the right to perform a compliance audit and to request a compliance audit from an independent, qualified third party, approved by the DOE-PMA.

The DOE-PMA shall reserve the right to require periodic and aperiodic inspections and audits of any DOE-RA facility within its domain to validate that the DOE-RA is operating in accordance with the security practices and procedures laid out in the DOE CPS.

The FBCA and the DOE Principal CA have the right to require periodic and aperiodic compliance audits or inspections of DOE Site CAs or DOE-RA operations to validate that the peer entities are operating in accordance with the security practices and procedures described in their respective CPS. Further, the Federal PKI PA has the right to require periodic compliance audits of the DOE Principal CA that interoperate with the FBCA under this CP. The Federal PKI PA shall state the reason for any a periodic compliance audit.

2.7.2 Identity/Qualifications of Compliance Auditor

The auditor shall have qualifications in accordance with best commercial practice and as mandated by law. The auditor must perform Certificate Authority or Information System Security Audits as its primary responsibility, and must be thoroughly familiar with this policy

and the applicable DOE Site CA's CPS. The DOE CPS must identify the internal compliance auditor for the applicable DOE Site CA.

2.7.3 Compliance Auditor's Relationship to Audited Party

The external compliance auditor for the DOE Principal CA or DOE Site CA's shall be a private firm that is independent from the DOE or any site contractor, or it shall be sufficiently organizationally separated from the audited CA to provide an unbiased, independent evaluation. The DOE-PMA shall determine whether a compliance auditor meets this requirement.

2.7.4 Topics Covered by Compliance Audit

The purpose of a compliance audit shall be to verify that the audited CA has in place a system to ensure the quality of the DOE certificate services that it provides, and that it complies with all of the requirements of this CP and its CPS. All aspects of the DOE PKI and DOE-RA operations related to this CP shall be subject to compliance audit inspections.

In addition, each MOA between the Federal PKI Policy Authority (FPKIPA) and the DOE PKI shall provide for a mechanism to confirm that CA is correctly implementing the MOA.

2.7.5 Actions Taken as a Result of Deficiency

Any discrepancies between the audited CA's operation, and the stipulations of its CPS and this policy must be noted. The DOE-PMA shall be immediately notified of all discrepancies. A remedy will be determined, including a time for completion.

Any remedy may include permanent or temporary cessation of the CA in question, 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 user community.

The DOE-PMA may determine that the audited CA is not complying with its obligations set forth in this CP or its respective CPS. When such a determination is made, the DOE-PMA may suspend operation of the CA in question, or may direct the DOE Principal CA to cease interoperating with the affected DOE Site CA (e.g., by revoking the certificate that the DOE Principal CA had issued to the DOE Site CA), or may direct that other corrective actions be taken which allow interoperation to continue. When the compliance auditor finds a discrepancy between how a CA is designed or is being operated or maintained and the requirements of this CP, the following actions shall be performed:

- DOE-PMA shall note the discrepancy,
- DOE-PMA shall notify the DOE Operational Authority of the discrepancy. If the discrepancy is judged by the DOE Operation Authority to be severe in nature (that is, it is determined to be a "material discrepancy" relative to the applicable requirements), the DOE Operational Authority shall notify the FPKI PA promptly, and;
- The party responsible for correcting the discrepancy shall determine what further notifications or actions are necessary pursuant to the requirements of this, and then proceed to make such notifications and take such actions without delay.

Depending upon the nature and severity of the discrepancy, and how quickly it can be corrected, the DOE Operational Authority may decide to temporarily halt operation of the CA in question, to revoke a certificate issued by that CA, or take other actions it deems appropriate. The DOE Operational Authority will develop procedures for making and implementing such determinations in coordination with the DOE-PMA.

2.7.6 Communication of Result

Reporting of results of an audit shall be communicated to the DOE Site CA, the DOE Principal CA, or user community Authority, and to the DOE-PMA, in accordance with this policy, and as defined by the applicable DOE CPS, and contract.

Any DOE Site CA found not to be in compliance with its CPS or this policy shall be notified immediately at the completion of the audit. Required remedies shall be defined and communicated to such a CA as soon as possible to limit the risks created. The implementation of remedies shall be communicated to the appropriate authority. A special audit may be required to confirm the implementation and effectiveness of the remedy.

2.8 Private and Sensitive Data

It is recommended that a certificate not contain information that is not necessary for its effective use, such that no sensitive information is contained therein. The DOE PKI may request non-certificate information to be used in managing the certificates within an organization. Such information may include identifying numbers, business or home addresses and telephone numbers. Collection of personal information may be subject to the Privacy Act of 1974 [PRIVACT]. Organizational information may be subject to the Freedom of Information Act [FOIACT] or other statutes. Other information may be subject to the Health Insurance Portability and Accountability Act (HIPAA), particularly in the case of OSHA. All information in DOE PKI records (not repository) shall be handled as sensitive, and access shall be restricted to those with official needs.

Except as specified in section 4.2.1, no person other than the subject of the corresponding certificate shall have access to a private signing key except as noted in section 6.2; it is recommended that the subject be prevented from viewing its keys in unencrypted form. Any private decryption keys held by the DOE Site CAs shall be held in strictest confidence. Under no circumstances shall any private key be stored unencrypted outside any DOE CA or DOE-RA's equipment. Any keys held by DOE Site CAs or DOE-RA's shall be released official in accordance with U.S. law and this policy (see section 2.3.3).

2.8.1 Types of Information Not Considered Private or Sensitive

None of the information included in a PKI repository should be considered sensitive or private. Repositories that contain sensitive information shall have approved access controls in place commensurate with the information to be protected.

2.8.2 Disclosure of Certificate Revocation/Suspension Information

Information concerning the revocation of a certificate or events leading to such a revocation should be limited to those involved. Notification of revoked certificates shall be placed on CRLs as per Section 4.4.3.

2.8.3 Release to Law Enforcement Officials

A DOE Site CA will release necessary information based on a court-authorized order that is duly signed by a competent judge of a court, in the course of a criminal investigation or discovery proceedings.

2.8.4 Disclosure Upon Owner's Request

No stipulation.

2.8.5 Other Information Release Circumstances

No stipulation.

2.9 Intellectual Property Rights

The U.S. Government retains exclusive rights to any products or information developed under or pursuant to this CP.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Initial Registration

3.1.1 Types of Names

Any DOE CA asserting this policy shall generate, sign, and process certificates that contain X.500 Distinguished Names (DNs). Domain Component (DC) naming may be part of the DN. If an Alternative Subject Name is assigned it must be marked non-critical.

3.1.2 Need for Names to Be Meaningful

The identity certificates issued pursuant to this CP are meaningful only if the names that appear in the certificates can be understood and used by Relying Parties. Names used in certificates must not only be unique and meaningful, but must also be consistent with a global DOE directory naming convention. Names used within the DOE PKI must identify the person or object to which they are assigned in a meaningful way. For people, this will typically be a legal name. For equipment, this may be a model name and serial number. Email addresses used as names should indicate an official relationship (e.g., an appropriate agency or corporate domain).

The DOE-PMA will establish an authority for the creation of Distinguished Names. It shall be called the DOE Naming Authority (DOE-NA). A DOE Site CA who uses DNs will coordinate with the DOE-NA to determine the proper elements for a given user. DNs shall represent the End Entity in a way that is easily understandable for humans. For equipment, this may be a model name and serial number, or an application process (e.g., Organization X Mail List or Organization Y Multifunction Interpreter). The CA shall use DNs in all certificates it issues.

Each DOE CAs asserting this policy shall only sign certificates with subject names from within a name-space approved by the DOE-PMA. In the case of the DOE Principal CA certifying DOE Site CAs, it must impose restrictions on the name space authorized in the peer DOE Site CA that are at least as restrictive as its own name constraints.

All certificates issued by the CA at the Medium Assurance level shall have name constraints asserted that limit the name space to that appropriate for their domains.

When technical means exist for imposing these constraints (such as the name constraints certificate extension), they shall be used. Otherwise, these constraints shall be imposed procedurally or contractually.

3.1.3 Rules for Interpreting Various Name Forms

Rules for interpreting name forms shall be contained in the applicable certificate profile and are established by the DOE-PMA and the DOE-NA.

3.1.4 Uniqueness of Names

Name uniqueness across the DOE PKI shall be enforced. The DOE Principal CA, DOE Site CAs and DOE-RAs shall enforce name uniqueness within the X.500 name space that they have

been authorized as set forth by the DOE-NA. Future name spaces will be directly approved by the DOE-NA. When other name forms are used, they too must be allocated such that name uniqueness across the DOE PKI is ensured, and they shall be approved in advance of use by the DOE-NA.

The DOE shall document in its CPS:

- Which name forms shall be used,
- How Site CAs will interact with the PCA, and;
- How CAs and RAs will allocate names within the End Entity community to guarantee name uniqueness among current and past End Entities.

3.1.5 Name Claim Dispute Resolution Procedure

The DOE-SRAAs shall investigate and correct if necessary any name collisions brought to its attention. If appropriate, a DOE-SRAA shall coordinate with and defer to the DOE-NA.

3.1.6 Recognition, Authentication, and Role of Trademarks

The DOE-SRAA will attempt to avoid the use of trademarks. The DOE-SRAA is not obligated to seek evidence of trademarks or court orders.

3.1.7 Method to Prove Possession of Private Key

In all cases where the user generates keys, the user is required to prove possession of the private key that corresponds to the public key in the request. Other mechanisms may also be acceptable.

In the case where key is generated directly on the End Entity's token, or in a key generator that benignly transfers the key to the End Entity's token, then the End Entity is in possession of the private key at the time of generation or transfer. If the user is not in possession of the token when the key is generated, then the token shall be delivered to the End Entity via an accountable method (see section 6.1.2).

When keyed hardware tokens are delivered to certificate subjects, the delivery shall be accomplished in a way that ensures that the correct tokens and activation data are provided to the correct subjects. The DOE must maintain a record of validation for receipt of the token by the subject. When any mechanism that includes a shared secret (e.g. PIN or password) is used, the mechanism shall ensure that the applicant and the Site Certification Authority, Registration Authority and/or Trusted Agent are the only recipients of this shared secret.

3.1.8 Authentication of Organization Identity

Requests for CA certificates in the name of the organization shall include the agency name, address, and documentation of the existence of the agency. The application shall be submitted, verified and approved by the PMA. Once approval is obtained from the PMA, the CAA or SRAA shall re-verify the information, in addition to the authenticity of the requesting representative and the representative’s authorization to act in the name of the organization.

3.1.9 Authentication of Individual Identity

For End Entities, DOE Site CAs or DOE-SRAAs shall ensure that the applicant's identity information is verified in accordance with this CP and the applicable CPS. The DOE Site CA, and/or DOE-RAs or DOE-SRAAs shall ensure that the applicant's identity information and public key are bound adequately. Additionally, the DOE Site CA, and/or DOE-RAs shall record and archive the process that was followed for issuance of each certificate. The process documentation shall include the following:

- The identity of the person performing the identification,
- A signed declaration by that person that he or she verified the identity of the End Entity as required by the applicable certificate policy,
- A unique identifying number from the ID of the verifier and, if in-person identity proofing is done, from the ID of the applicant,
- The date and time of the verification, and;
- A declaration of identity which shall be signed with a handwritten signature (collected at the time of initial employment) by the certificate applicant; if in-person identity proofing is done, this shall be performed in the presence of the person performing the identity authentication. Where the applicant is not a human being but is instead a network device or some other entity, the requirements pertaining to identity proofing shall be done through the human owner or designated representative.

Identity shall be established by in-person proofing before the DOE-SRAA, Trusted Agent or an entity certified by the DOE as being authorized to confirm identities. The information provided shall be verified to ensure legitimacy. A trust relationship between the Trusted Agent and the applicant that 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 (e.g. Department of Energy badge), or two non-Federal Government IDs, one of which must be a photo ID (e.g. drivers license).

For All Levels of Assurance: If an Applicant is unable to perform face-to-face registration alone, the applicant shall be represented by a trusted person already issued a digital certificate by the Agency. 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.

3.1.10 Authentication of Component Identities

Some computing and communications components (routers, firewalls, etc.) will be named as certificate subjects (end entities). In such cases, the component must have a human Sponsor that has been issued a digital certificate by the DOE Site CA. The Sponsor is responsible for providing the following registration information:

- Equipment identification,

- Equipment name that conforms to the DOE-NA naming convention for such End Entities,
- Equipment public keys,
- Equipment authorizations and attributes (if any are to be included in the certificate),
- Contact information to enable the DOE Site CA or DOE-SRAA to communicate with the Sponsor when required, and;
- Any other information required by protocols used (such as CEP – the Certificate Enrollment Protocol).

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 3.1.9.

3.2 Certificate Renewal, Update, and Routine Re-key

The procedures for accomplishing End Entity Certificate Renewal, Update and Routine Re-Key specified in the Certificate Policy will be detailed in the DOE CPS.

3.2.1 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 an End Entity periodically obtains new keys and re-establishes its identity. Re-keying a certificate means that a new certificate is created that is identical to the old one, except that the new certificate has new, different public keys (corresponding to a new, different private keys); a different certificate serial number; and may be assigned a different validity period.

Re-key of the End Entities at the DOE Site CAs shall be accomplished at three (3) years for a signing certificate and two (2) years for an encryption certificate, from the time of initial registration. End Entities will be authenticated either by: (a) performing the initial registration identification process defined in Section 3.1, or (b) using the currently valid signing key issued to the End Entity by the DOE Site CA.

End Entity identities shall be re-established through the initial registration process at least once every three years from the time of initial registration.

New certificates will need to be issued to the DOE Site CAs when the DOE Principal CA re-keys.

3.2.2 Certificate Renewal

Renewing a certificate means creating a new certificate with the same name, key, and authorizations as the old one, but a new, extended validity period and a new serial number. Certificates may be renewed in order to minimize the size of CRLs. 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 End Entity name and attributes are unchanged. Thus, the DOE Site CAs may renew certificates good for one year, renew it twice (each for a one year period), and then re-key at the end of the third year. But, in no case shall the certificate validity period be extended beyond a public key's original validity period.

3.2.3 Certificate Update

Updating a certificate means creating a new certificate that has the same or a different key and a different serial number, and that it differs in one or more other fields, from the old certificate. For example, a Site CA may choose to update a certificate of a Subscriber whose characteristics have changed (e.g., has just received a medical degree). The old certificate may or may not be revoked, but must not be further re-keyed, renewed, or updated.

Further, if an individual's name changes (e.g., due to marriage), then proof of the name change must be provided to the RA or other designated agent (as set forth above) in order for an updated certificate having the new name to be issued.

Finally, when a CA updates its private signature key and thus generates a new public key, the CA shall notify all CAs, RAs, and subscribers that rely on the CA's certificate that it has been changed. For self-signed ("root") certificates, such certificates shall be conveyed to users in a manner consistent with the medium assurance level to preclude malicious substitution attacks.

3.3 Obtaining a New Certificate After Revocation

In the event of certificate revocation, issuance of a new certificate shall always require that the party go through the initial registration process per Section 3.1 above.

3.4 Revocation Request

Revocation requests must be authenticated. User requests to revoke a certificate may be authenticated using that certificate's associated private key, if available, regardless of whether or not control of the private key is in doubt.

4 OPERATIONAL REQUIREMENTS

4.1 Application for a Certificate

It is not the intent of this policy to impose implementations on CAs or users, but to identify the required information and procedures that constitute assurance and support trust in the DOE PKI. The following procedures satisfy the security requirements of this document; particular mechanisms or the sequencing of operations may be decided by the DOE-PMA or issuing DOE Site CAs.

The following steps are required of a user when applying for a certificate:

- Establish need for certificate,
- Establish identity of subject (per Section 3.1.9),
- Obtain public/private key pairs for each certificate required,
- Prove to the DOE-RA or DOE Site CA that the public key forms a functioning key pair with the private key held by the user (per Section 3.1.7),
- Provide a point of contact for verification of any roles or authorizations requested, and;
- A knowledge receipt of the certificate and responsibilities via signed Subscribers Agreement.

CAs implementing this CP shall certify other CAs (to include cross-certification) only as authorized by the DOE-PMA.

4.1.1 Delivery of Public Key to Certificate Issuance

Public keys must be delivered to the certificate issuer in a way that binds the applicant's verified identification to the public key being certified. This binding must be accomplished using cryptography at least as strong as that employed in certificate issuance. Additionally, the binding may also be accomplished using non-cryptographic physical and procedural mechanisms. These mechanisms may include, but are not limited to, floppy disk (or other storage medium) sent via registered mail or courier, or by delivery of a token to a certificate issuer for local key generation at the point of certificate issuance or request. The methods used for public key delivery shall be stipulated in the DOE CPS.

In those cases where public/private key pairs are generated by the DOE Site CA on behalf of the End Entity, the DOE Site CA shall implement security control mechanisms to ensure that the token on which the public/private key pair is held is sent to the proper End Entity in a manner commensurate with the medium assurance level, and that the token is not activated prior to receipt by the proper End Entity.

4.2 Certificate Issuance

Upon receiving a request for a certificate from an applicant, the DOE Site CAA, or DOE-SRAA shall respond in accordance with the requirements set forth in this CP and its CPS.

The certificate request may contain an already built ("to-be-signed") certificate. This certificate will not be signed until the processes set forth in the DOE CP (Section 6) and the relevant DOE Site CPS have been met.

While the End Entity may do most of the data entry, it is still the responsibility of the DOE-SRAA to verify that the information is complete and accurate. This may be accomplished either through a system approach linking trusted databases containing personnel information or through personal contact with the End Entity's organization. If databases or other equivalent authentication verification methods are used to confirm End Entity 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 request, DOE Site CAs shall:

- Verify the identity of the requestor,
- Verify the authority of the requestor and the integrity of the information in the certificate request,
- Build and sign a certificate if all certificate requirements have been met, and;
- Make the certificate available to the End Entity.

4.2.1 Delivery of End Entity's Private Key to End Entity

A private key that is generated will remain within the cryptographic boundary of the cryptographic module. If the owner of the module generates the key, then here is no need to deliver the private key. If the key is generated elsewhere, then the cryptographic token must be delivered to the End Entity. Accountability for the location and state of the cryptographic token must be maintained until it is in the possession of the End Entity. The End Entity shall acknowledge receipt of the cryptographic token. Under no circumstances shall anyone other than the End Entity have knowledge of or control over private signing keys. Anyone who generates a private signing key for an End Entity shall not escrow any copy of the key. Hardware tokens containing DOE Site CA and DOE-SRAA private signature keys may be backed-up subject to the security audit requirements of Section 4.5.

Normally, a certificate shall be issued to a single End Entity. For cases where there are several persons 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 End Entities. In these cases:

- An information systems security office or equivalent shall be responsible for ensuring control of the private key, including maintaining a list of End Entities who have access to use of the private key, and accounting for which End Entity had control of the key at what time,

- The list of those holding the shared private key must be provided to, and retained by, the applicable CA or designated representative(s), 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 End Entity obligations).

4.2.2 End Entity's Public Key Delivery and Use

The public key of the DOE Site CA must be available for trusted certification links to be created and verified. To extract the key from a certificate with confidence that it has not been altered, the DOE Site CA must ensure that its users have its self-signed principal certificate in a trustworthy form. Such a self-signed principal certificate is sometimes called a Trusted Certificate. Acceptable methods for Trusted Certificate delivery include, but are not limited to:

- The DOE Site CA loading a trusted Certificate onto tokens delivered to relying parties via appropriate mechanisms for the medium assurance level,
- Protected distributions of Trusted Certificates through out-of-band mechanisms,
- Comparison of certificate hashes or fingerprints against Trusted Certificate hashes or fingerprints made available via authenticated out-of-band sources (note that fingerprints or hashes posted in-band along with the certificate are not acceptable as an authentication mechanism),
- Loading certificates from Web sites protected with a currently valid certificate of equal-or-greater assurance level than the certificate being downloaded, and;
- Transmission over an authenticated encrypted link with the CA.

4.3 Certificate Acceptance

While certificates issued by the DOE PKI are U.S. Government property, individual users may be liable for actions taken with the certificate (i.e., private key).

Before a DOE Site CA allows an End Entity to make effective use of its private key, the DOE Site CA shall:

- Explain to the End Entity its responsibilities as defined in Section 2.1.5,
- Inform the End Entity of the creation of a certificate and the contents of the certificate,
- Require the End Entity to acknowledge his or her obligations respecting protection of the private key and the use of the certificate, and;
- Documents the End Entity's acceptance of its responsibilities and the certificate via the Subscribers Agreement (which requires compliance with this CP and protection of the private keys but is commensurate with the medium assurance level) .

The ordering of this process, and the mechanism used, will depend on factors such as where keys are generated and how certificates are posted. In the case of non-human components (router, firewalls, etc.), the PKI Sponsor shall perform the functions of the End Entity.

4.4 Certificate Suspension and Revocation

4.4.1 Circumstances for Revocation

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

- Identifying information or affiliation components of any names in the certificate become invalid,
- Privilege attributes (if any) asserted in the End Entity's certificate are reduced,
- The End Entity can be shown to have violated, or is suspected of violating, the requirements of the DOE CP or its End Entity agreement, and;
- The End Entity or other authorized party (as defined in the DOE CPS) asks for their certificate to be revoked.

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 expires.

4.4.1.1 Who Can Request Revocation of a Certificate Issued by a DOE Site CA

Within the DOE PKI, a DOE Site CA may summarily revoke certificates within its domain as set forth in the relevant DOE Site CPS. Where practicable, written notice and brief explanation for the revocation shall be provided to the End Entity. A DOE-SRAA can revoke a certificate on behalf of any authorized party as specified in the DOE CPS. An End Entity can initiate a revocation request for its own certificate.

4.4.1.2 Procedure for Revocation Request

An End Entity may request revocation of its own certificate using any format that identifies the certificate to be revoked, explains the reason for revocation, and allows the request to be authenticated (e.g. digitally or manually signed). The steps involved in the process of requesting a certificate revocation shall be detailed in the relevant DOE Site CPS.

Authentication of certificate revocation requests is important to prevent malicious revocation of certificates by unauthorized parties. When revocation is being requested for reason of key compromise or suspected fraudulent use, the End Entity's request or the DOE-SRAA's revocation request must so indicate. If a DOE-SRAA performs this on behalf of an End Entity, a formal, signed message format known to the DOE Site CA shall be employed. All requests shall be authenticated; for signed requests from the certificate subject, or from a DOE-SRAA, verification of the signature is sufficient.

Upon receipt of a revocation request from the End Entity or another authorized party, the DOE-SRAA shall authenticate the revocation request. A DOE-SRAA may, at its discretion, take reasonable measures to verify the need for revocation. If the revocation request appears to be valid, the DOE Site CA shall revoke the certificate by placing its serial number and other identifying information on a CRL, in addition to any other revocation mechanisms used.

For PKI implementations using hardware tokens, an End Entity ceasing its relationship with an organization that sponsored the certificate shall, prior to departure, surrender to the organization (through any accountable mechanism) all cryptographic hardware tokens that were issued by or on behalf of the sponsoring organization. If an End Entity leaves an organization and the hardware tokens cannot be obtained from the End Entity, then all End Entities' certificates associated with the un-retrieved tokens shall be immediately revoked. The token shall be zeroized or destroyed promptly upon surrender and shall be protected from malicious use between surrender and zeroization or destruction.

4.4.1.3 Revocation Request Grace Period

There is no revocation grace period under this policy; the DOE PKI shall revoke certificates as quickly as practical upon receipt of a proper revocation request and shall always revoke certificates within the time constraints described in Section 4.4.3.1.

4.4.2 Suspension

The DOE PKI will not support suspension of certificates.

4.4.3 Certificate Revocation Lists (CRL)

4.4.3.1 CRL Issuance Frequency

Certificate Revocation Lists (CRLs) shall be issued at least once within a 24-hour period, even if there are no changes to be made, to ensure timeliness of information. The exception to this is the CRL issued by the PCA, which must be issued at least once every 28 days. CRLs may be issued more frequently than required; if there are circumstances under which the CA will post early updates, these shall be spelled out in the CA's respective CPS. The CA shall ensure that superseded CRLs are removed from the repository upon posting of the latest CRL. There are no CRL issuance frequency requirements except for reasons of key compromise or loss as set forth above. If the CRL is being issued as a result of a loss or compromise of a private key, the CRL must be issued within 18 hours of notification, this requirement also applies to the DOE PCA. CAs shall make public a description of how to obtain revocation information for the certificates they publish, and an explanation of the consequences of using dated revocation information. This information shall be given to End Entities during certificate request or issuance, and shall be readily available to any potential relying party.

4.4.3.2 CRL Checking Requirements

Use of revoked certificates could have damaging or catastrophic consequences in certain applications. The matter of how often new revocation data should be obtained is a determination

to be made by Relying Party, considering the risk, responsibility and consequences for using a certificate whose revocation status cannot be guaranteed.

4.4.4 On-line Revocation/Status Checking Availability

Relying Party client software may optionally support on-line status checking. Thus, client software using on-line revocation checking need not obtain or process CRLs. The DOE-PMA will determine when and under what circumstances DOE Site CAs will provide on-line status checking of DOE Site CA certificates.

4.4.5 Other Forms of Revocation Advertisements Available

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

4.4.6 Checking Requirements for Other Forms of Revocation Advertisements

CAs supporting other forms of revocation will specify availability and checking requirements in their CPS.

4.4.7 Special Requirements Related to Key Compromise

In the event that a DOE Site CA's private key is compromised or lost, the DOE Site CA shall publish a CRL at the earliest feasible time.

4.5 Security Audit Procedure

Stipulations in this section that refer to all DOE CA audits shall be construed as referring to DOE-RA audits as well, to the extent that DOE-RA equipment is used for the purposes and processes the data described. Audit log files shall be generated for all events relating to the security of the DOE PKI. 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 created and maintained in accordance with Retention Period for Archive, Section 4.6.2.

4.5.1 Types of Events Recorded

All DOE CAs shall record events identified in the National Institute of Standards and Technology (NIST) developed Certificates Issuing and Management Components (CIMC) Protection Profile for Level 2 components[1]. All security auditing capabilities of each DOE CAs

[1] http://cs-www.ncsl.nist.gov/pki/documents/CIMC_PP_20011031.pdf

operating system and DOE PKI applications shall be enabled during installation.. At a minimum, each audit record shall include the following (either recorded manually or automatically for each auditable event):

- Type of event,
- Date and time the event occurred,
- Success or failure indicator when executing the CAs signing process,
- Success or failure indicator when performing certificate revocation; and,
- Identity of the entity and/or operator that caused the event.
- A message from any source requesting action by a DOE Site CA is an auditable event; the message must include date, time, source, destination and contents.

The table below represents the event auditing. Those auditable events that are provided by the DOE CAs operating system and DOE PKI applications will be represented in a collection of audit logs for a Site CA.

Table 4.5.1-1 Auditable Events

Auditable Event	Audited
SECURITY AUDIT	
Any changes to the Audit parameters, e.g., audit frequency, type of event audited	X
Any attempt to delete or modify the Audit logs	X
AUTHENTICATION	
Successful and unsuccessful attempts to assume a role	X
Change in the value of maximum authentication attempts	X
Maximum number of unsuccessful authentication attempts during user login	X
An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts	X
An Administrator changes the type of authenticator, e.g., from password to biometric	X
KEY GENERATION	
Whenever the DOE Principal CA or a DOE Site CA generates a key. (Not mandatory for single session or one-time use symmetric keys)	X
PRIVATE KEY LOAD AND STORAGE	
The loading of component private keys	X
All access to certificate subject private decryption keys retained within the DOE Principal CA or a DOE Site CA for key recovery purposes	X

Auditable Event	Audited
TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE	
All changes to the trusted public keys, including additions and deletions	X
PRIVATE KEY EXPORT	
The export of private keys (keys used for a single session or message are excluded)	X
CERTIFICATE REGISTRATION	
All certificate requests	X
CERTIFICATE REVOCATION	
All certificate revocation requests	X
CERTIFICATE STATUS CHANGE APPROVAL	
The approval or rejection of a certificate status change request	X
FBCA OR AGENCY CA CONFIGURATION	
Any security-relevant changes to the configuration of the DOE Principal CA or a DOE Site CA	X
ACCOUNT ADMINISTRATION	
Roles and users are added or deleted	X
The access control privileges of a user account or a role are modified	X
CERTIFICATE PROFILE MANAGEMENT	
All changes to the certificate profile	X
REVOCATION PROFILE MANAGEMENT	
All changes to the revocation profile	X
CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT	
All changes to the certificate revocation list profile	X
MISCELLANEOUS	
Installation of the Operating System	X
Installation of the DOE Principal CA or a DOE Site CA	X
Installing hardware cryptographic modules	X
Removing hardware cryptographic modules	X
Destruction of cryptographic modules	X
System Startup	X

Auditable Event	Audited
Logon attempts to DOE Principal CA or a DOE Site CA Apps	X
Receipt of Hardware / Software	X
Attempts to set passwords	X
Attempts to modify passwords	X
Backing up DOE Principal CA or a DOE Site CA internal database	X
Restoring DOE Principal CA or a DOE Site CA internal database	X
File manipulation (e.g., creation, renaming, moving)	X
Posting of any material to a repository	X
Access to DOE Principal CA or a DOE Site CA internal database	X
All certificate compromise notification requests	X
Loading tokens with certificates	X
Shipment of tokens	X
Zeroizing tokens	X
Re-key of the DOE Principal CA or a DOE Site CA	X
Configuration changes to the CA server involving:	
Hardware	X
Software	X
Operating System	X
Patches	X
Security Profiles	X
PHYSICAL ACCESS / SITE SECURITY	
Personnel Access to room housing DOE Principal CA or a DOE Site CA	X
Access to the DOE Principal CA or a DOE Site CA server	X
Known or suspected violations of physical security	X
ANOMALIES	
Software Error conditions	X
Software check integrity failures	X
Receipt of improper messages	X
Misrouted messages	X
Network attacks (suspected or confirmed)	X

Auditable Event	Audited
Equipment failure	X
Electrical power outages	X
Uninterrupted Power Supply (UPS) failure	X
Obvious and significant network service or access failures	X
Violations of Certificate Policy	X
Violations of Certification Practice Statement	X
Resetting Operating System clock	X

4.5.2 Frequency of Processing Data

Audit logs shall be reviewed at least once every two months. All significant events shall be explained in an audit log summary. 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 in the logs. Actions taken as a result of these reviews shall be documented in a report which will be provided to the PMA upon request.

A statistically significant set of security audit data generated by each 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. At least 20% of the security audit data generated by each CAs since the last review shall be examined, at a minimum, once every two months.

4.5.3 Retention Period for Security Audit Data

Audit logs shall be retained onsite for at least two months as well as being retained in the manner described below or in accordance with NARA, which ever is greater. The individual who removes audit logs from a DOE Site CA system shall be an official different from the individuals who, in combination, command the DOE Site CA's signature key. The name of the personnel role will be identified in the applicable DOE CPS.

4.5.4 Protection of Security Audit Data

The audit process shall be done by the DOE Security Officer (DOE-SO) under the control of the DOE Operational Authority. DOE system configuration and procedures must be implemented together to ensure that:

- Only authorized people have read access to the logs,
- Only authorized people may archive or delete 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 deletion or destruction prior to the end of the audit log retention period (note that deletion requires modification access). Audit logs shall be moved to a safe, controlled storage location separate from the DOE Site CA equipment.

4.5.5 Security Audit Data Backup Procedures

Audit logs and audit summaries shall be backed up at least monthly. A copy of the audit log shall be stored remotely in accordance with the DOE CPS on a monthly basis.

4.5.6 Security Audit Collection System (Internal vs. External)

The audit log collection system may or may not be external to the DOE Site CA. The audit process shall not be done by or under the control of the DOE CAA. Audit processes shall be invoked at system startup, and cease only at system shutdown. Should it become apparent that an automated audit system has failed, and the integrity of the system or confidentiality of the information protected by the system is at risk, then the DOE Operational Authority shall determine whether to suspend the DOE Site CA until the problem is remedied.

4.5.7 Notification to Event-Causing Subject

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

4.5.8 Vulnerability Assessments

The Operational Authority will perform periodic self-assessments of security controls.

4.6 Records Archival

4.6.1 Types of Events Archived

DOE Site CA archive records shall be detailed enough to establish the validity of a certificate at a specific point in time as set forth in section 4.6.1. At a minimum, the following data shall be archived.

The following data shall be recorded for archive at the initialization of the DOE Site CA equipment:

Table 4.6.1-1 Archived Events

Data To Be Archived	Archived
DOE Site CA accreditation (if necessary)	X

Data To Be Archived	Archived
Certification Practice Statement	X
Contractual obligations (including any contractual agreements to which the DOE Site CA is bound)	X
DOE Site CA System and equipment configuration	X
Modifications and updates to DOE Site CA system equipment or configuration	X
Certificate requests	X
Revocation requests	X
End Entity identity Authentication data as per Section 3.1.9	X
Documentation of receipt and acceptance of certificates	X
Documentation of receipt of tokens	X
All certificates issued or published	X
Private Decryption Keys	X
Record of DOE CA re-key	X
Security of audit data	X
All CRLs issued and/or published	X
All Audit Logs	X
Other data or applications to verify archive contents	X
Documentation required by compliance auditors	X

4.6.2 Retention Period for Archive

Archive records will be kept for as long as the PKI is operational or to meet with NARA guidelines, whichever is longer. Applications required to process the archive data shall also be maintained for as long as necessary as determined by the DOE Operational Authority or to meet

with NARA guidelines, whichever is longer. If the original media cannot retain the data for the required period, a program to periodically transfer the archived data to new media shall be defined by the archive site.

4.6.3 Protection of Archive

No unauthorized user shall be permitted to write to, modify, or delete the archive. For the any DOE CA, archived records may be moved to another medium when authorized by the DOE-PMA. The contents of the archive shall not be released except as determined by the DOE-PMA or as required by law. Records of individual transactions may be released upon request of any End Entities involved in the transaction or their legally recognized agents. Archive media shall be stored in a safe, controlled storage facility separate from the applicable CA.

The archive records shall be time-stamped by those archive subsystems that support time stamping of records. Archive media shall be stored in a safe, controlled storage facility separate from the applicable CA. Procedures for archiving can be found in the CPS.

4.6.4 Archive Backup Procedures

No stipulation.

4.6.5 Requirements for Time-Stamping of Records

No stipulation.

4.6.6 Archive Collection System (Internal or External)

No stipulation.

4.6.7 Procedures to Obtain and Verify Archive Information

Procedures detailing how to create, package and send the archive information shall be published in the relevant DOE Site CPS. Only authorized users will be allowed to access the archive.

4.7 Key Changeover

To minimize risk from compromise of a DOE Site CA's private signing key, that key may be changed often. Authorities may not issue certificates that extend beyond the expiration dates of their own certificates and public keys; therefore, their certificate Validity periods must be greater than those for users, listed in section 3.2. To minimize risk to the PKI through compromise of an Authority's key, those keys will be changed more frequently, and only the new key will be used for Authority signing purposes from that time. The older certificate will be available to verify old signatures. The CAs signing key shall have a validity period as described in section 6.3.2.

4.8 Compromise and Disaster Recovery

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

If any DOE CA equipment or software is damaged or rendered inoperative, but the CA's signature keys are not destroyed, that CA's operation shall be reestablished as quickly as possible, giving priority to the ability to generate CRLs.

4.8.2 DOE Principal CA Signature Keys are Revoked

If the DOE Principal CA cannot issue a CRL for a period of seven calendar days, the DOE-PMA must report its keys as compromised and reestablish revocation capabilities as quickly as possible in accordance with procedures set forth in the respective CPS. The FBCA PKI Policy Authority shall be notified as soon as possible.

4.8.3 DOE Principal CA Signature Keys are Compromised

If the DOE Principal CA signature keys are compromised or lost (such that compromise is possible even though not certain), the DOE-PMA and the FBCA shall be securely and immediately notified in a manner consistent with the medium assurance level (so that certificates issued by and any cross-certificates issued to the DOE Principal CA can be revoked), a CRL shall be immediately published as set forth above, a new DOE Principal CA key pair shall be generated in accordance with procedures set forth in this CP, and new DOE Site CA certificates shall be issued in accordance with this CP and the relevant CPS(s). The DOE PKI shall also investigate and report to the DOE-PMA what caused the compromise or loss, and what measures have been taken to preclude recurrence.

4.8.4 DOE Computing Facilities Impaired After a Natural or Other Type of Disaster

In the case of a disaster whereby any DOE CA installation is physically damaged and all copies of a DOE Site CA or DOE Principal CA signature key are destroyed as a result, the DOE-PMA shall be immediately notified in a manner consistent with the medium assurance level, and the DOE-PMA shall take whatever action it deems appropriate. The affected installation shall then be completely rebuilt, by reestablishing the CA equipment, generating new private and public keys, being re-certified, and re-issuing all cross certificates. Relying parties may decide of their own volition whether to continue to use certificates signed with the destroyed private key pending reestablishment of CA operation with new certificates.

4.9 DOE CA Termination

In the event of termination of any DOE CA, certificates signed by the CA shall be revoked and the DOE-PMA shall advise agencies that have entered into MOAs with the DOE-PMA that CA operation has terminated so they may revoke certificates they have issued to the relevant DOE CA. Prior to termination of any DOE CA, the DOE PKI shall provide archived data to a DOE-PMA approved archive facility.

5 PHYSICAL, PROCEDURAL AND PERSONNEL SECURITY CONTROLS

In the community covered by this CP (see section 1.3), CAs, RAs and end entities operate in a DOE environment; therefore, in addition to the requirements of this section, all DOE requirements for operation must be met. This shall be so stated in the supporting CPS(s).

Where security measures and controls indicated below are already in place as part of existing DOE policy, site security policy, computer protection plans, or other applicable policy, these policies shall be cited in the CPS.

5.1 Physical Controls for DOE CAs and RAs

The DOE PKI shall impose physical security requirements that provide similar levels of protection as those specified below. All the physical control requirements apply equally to all DOE CAs and associated RA equipment.

All DOE CA and RA equipment shall be protected from unauthorized access while the cryptographic module is installed and activated. All DOE CA and RA equipment 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 specific DOE CA and RA equipment environment. All DOE CA and RA cryptographic tokens shall be protected at all times against theft, loss and unauthorized use.

5.1.1 Site Location and Construction

The location and construction of the facility housing any DOE CA equipment shall be consistent with facilities used to house medium value, sensitive information requiring medium assurance level as defined by NIST and NSA. 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 equipment and records.

5.1.2 Physical Access

All DOE CA equipment shall always be protected from unauthorized access, 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. Since the DOE plans to issue certificates at a Medium Assurance level, all DOE site CAs shall satisfy the requirements for a medium security zone, be manually or electronically monitored for unauthorized intrusion at all times, ensure no unauthorized access to any DOE CA server is permitted, ensure a site access log is maintained and inspected periodically, require a physical access controls commensurate with the medium assurance level to both the cryptographic module and computer system, and ensure all removable media and paper containing sensitive plain-text information are stored in containers appropriate for protecting

these data. Access lists will be clearly and visibly posted outside all doors and entrances leading to any DOE CA equipment.

Removable cryptographic modules shall be inactivated prior to storage. When not in use, removable cryptographic modules, and any activation information used to access or enable cryptographic modules, all DOE CA equipment shall be placed in approved, locked containers or a vault type room sufficient for housing equipment and information commensurate with the sensitivity or value of the information being protected by the certificates issued by the relevant DOE CA. Activation data shall either be memorized, or recorded and stored in a manner commensurate with the security afforded the cryptographic module, and shall be separated in storage from the cryptographic module.

A security check of the facility housing any DOE CA equipment 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 "open", and protected when "closed"; and for the DOE Principal CA, that all equipment other than the directory is shut down),
- Any security containers are properly protected,
- Physical security systems (e.g., door locks, vent covers) are functioning properly, and;
- The area is protected against unauthorized access.

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 and clearly posted. All persons in this group shall have met all of the personnel controls stated in Section 5.3 of this CP. 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. No individual shall enter or remain in the facility housing the CA equipment alone. Two-person physical access control to both the cryptographic module and computer system is required for the CA. Therefore at least two persons shall be present at all times. The facility housing RA equipment shall not require the presence of two persons except at startup and shut down. All maintenance shall be monitored by at least one Operational Authority personnel when performed on site. Equipment sent off site for maintenance at approved facilities shall be tested and certified by the Operational Authority to ensure that only authorized software and hardware are installed prior to being put back into operation. No keys shall be stored on any system that is being sent off site for maintenance.

5.1.3 Electrical Power

The facility that houses any DOE CA shall be supplied with power and air conditioning sufficient to create a reliable operating environment. In addition, personnel areas within the facility shall be supplied with sufficient utilities to satisfy operational, health, and safety needs. DOE CAs and DOE CA directories shall have backup power capability sufficient to automatically lockout input, finish any pending actions, and record the state of the equipment before lack of power or air conditioning causes a shutdown.

5.1.4 Water Exposures

No stipulation.

5.1.5 Fire Prevention and Protection

No stipulation.

5.1.6 Media Storage

All DOE CA media shall be stored so as to protect it from accidental damage (water, fire, electromagnetic). Media that contains audit, archive, or backup information shall be duplicated and stored in a location separate from the relevant DOE CA. Media storage shall also comply with National Archives and Records Administration (NARA) guidelines and DOE record retention policies.

5.1.7 Waste Disposal

No stipulation.

5.1.8 Off-site Backup

Full system backups, sufficient to recover from system failure, shall be made on a periodic schedule, described in the DOE CPS. Backups are to be performed and stored off-site not less than once per week. At least one backup copy shall be stored at a remote location (separate from the relevant DOE CA equipment). Only the latest backup need be retained. The backup shall be stored at a site with physical and procedural controls commensurate to that of the operational DOE CA.

5.2 Procedural Controls for DOE CAs

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 and above reproach. The functions performed in these roles form the basis of trust for all uses of the DOE PKI. Two approaches are taken to increase the likelihood that these roles can be successfully carried out. The first ensures that the person filling the role is trustworthy and properly trained. The second distributes the functions among more than one person, so that any malicious activity would require collusion.

The trusted roles explicitly defined by this DOE CP include the CA Administrator (DOE-CAA), Registration Authority Administrators (DOE-SRAAs), DOE System Administrator (DOE-SA) and DOE Security Officer (DOE-SO). All roles, with the exception of the DOE-SA, are appointed by the site Operational Authority. For the DOE Site CAs, the trusted roles shall be performed as described below. The DOE-CAAs and/or DOE-SRAAs may identify other trusted

individuals within their Certification Practice Statement responsible for performing some of the responsibilities identified below.

The table below maps DOE Trusted Roles to the FBCA Trusted Roles as specified in the *X.509 Certificate Policy for the Federal Bridge Certification Authority (FBCA*), dated September 10th, 2002.

FBCA Trusted Role	DOE Trusted Role
Administrator	Certification Authority Administrator (CAA)
Officer	Site Registration Authority Administrator (SRAA)
Auditor	Security Officer (SO)
Operator	System Administrator (SA)

5.2.1.1 DOE-CAA

The primary responsibilities of the CAA include:

- Installation, configuration, and maintenance of a DOE CA,
- Establishing and maintaining DOE CA PKI software accounts,
- Configuring certificate profiles or templates and audit parameters,
- Generating and backing up DOE CA keys, and;
- Establishing an Operational Authority approved system of written log books and other written records as needed to control access to equipment; ensuring that this list of log books and the operational procedures necessary for maintaining them are published in the CPS; and, performing periodic checks to ensure that all personnel are following these procedures.

CAAs do not issue certificates to End Entities except under circumstances that are approved by the site Operational Authority.

5.2.1.2 DOE-SRAA

Any DOE-RA or DOE-SRAA that operates under this policy is subject to the stipulations of this policy. The DOE-SRAA's role and the corresponding procedures shall be defined in a CPS. The DOE-SRAA's responsibility is to ensure that following functions occur according to the stipulations of this policy:

- Registering new End Entities and requesting the issuance of certificates,
- Entering information into the registration system and verifying its accuracy,

- Verifying the identity of End Entities and the 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 DOE-SA

The DOE CPS and agency specific guidelines, procedures, or practice statements shall define all of the trusted roles for the DOE-SA for proper, safe and operation of DOE CA equipment and procedures. The responsibilities include:

- Initial configuration of DOE CA equipment, including the installation of the applications, initial setup of accounts, configuration of initial host and network interface
- Creating devices to support recovery from catastrophic system loss,
- Performing system backups, software upgrades and recovery, and;
- Modifying host and/or network interface configuration.

5.2.1.4 DOE-SO

The DOE CPS and agency specific guidelines, procedures, or practice statements shall define the responsibilities of the DOE-SO (DOE Security Officer) to ensure that the operation of DOE CA equipment and procedures is commensurate with the medium assurance level. The responsibilities include:

- Performing or overseeing the performance of an internal compliance audit,
- Performing or overseeing proper storage and distribution of backups and upgrades to an offsite location,
- Auditing security privileges and access control of individuals authorized to operate a DOE CA or its directory,
- Overseeing archive and deletion functions of the audit logs, and;
- Reviewing audit logs.

5.2.2 Separation of Roles

Individual trusted personnel shall be specifically designated to the four roles defined in section 5.2.1 above. A DOE-SO cannot assume any other Trusted Role. Individuals who assume a DOE-SRAA role may never assume a DOE-SA role. A DOE-CAA cannot assume a DOE-SRAA role, and vice-versa. DOE CA software shall identify and authenticate its users. No individual shall be assigned more than one identity, e.g. a person cannot possess two certificates with different Distinguished Names (See section 7.1.4).

5.2.3 Number of Persons Required Per Task

To best ensure the integrity of DOE CA equipment and operation, separation of roles shall be implemented as specified in section 5.2.2. The separation provides a set of checks and balances over DOE CA operation. Under no circumstances shall the incumbent of a DOE CA role perform its own auditor function.

5.2.4 Identification and authentication for each role

An individual shall identify and authenticate him/herself before being permitted to perform any actions set forth above for that role or identity.

5.3 Personnel Controls

5.3.1 Background, Qualifications, Experience, and Security Clearance Requirements

All persons filling trusted roles shall be selected on the basis of loyalty, trustworthiness, and integrity, and must be U.S. citizens. DOE-CAAs shall hold a minimum of a DOE "L" clearance[2]. DOE-SRAA personnel shall hold "L" clearance or agency equivalent security clearances unless a waiver is granted by the DOE-PMA. Staffing at some remote DOE locations may preclude DOE-SRAAs from being U.S. citizens or possessing "L" clearance clearances. In this case, a waiver from the DOE-PMA may be granted on a case-by-case basis. Additionally, in some exceptional cases, government employees from government agencies other than DOE may perform RAA functions. Here also, a waiver from the DOE-PMA may be granted on a case-by-case basis. The DOE Information Technology Center (ITC) Director shall be responsible and accountable for the operation of all DOE CAs.

The requirements governing the qualifications, selection, and oversight of individuals who operate, manage, oversee, and audit a particular DOE CA shall be set forth in the applicable CA's CPS.

Candidates for trusted roles shall be appointed in writing by an individual to be specified in the applicable CAs CPS attesting to the fact that they meet the requirements set forth in this section.

5.3.2 Background Check Procedures

Agency procedures shall be followed to determine the need for and extent of background checks. Such checks are to be performed solely to determine the suitability of a person to fill a DOE CA trusted role. Background check procedures shall be described in the DOE CPS and agency specific guidelines, procedures, or practice statements. Such checks are to establish, but are not limited to, the fulfillment of all requirements in Section 5.3 of this CP and of the DOE CPS.

[2] We should give an idea of what an "L" clearance maps to in DOD terms for people external to DOE's knowledge.

5.3.3 Training Requirements

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

- CA/RA and RAA security principals and mechanisms,
- All PKI software versions in use on the DOE CA system,
- All PKI duties they are expected to perform, and;
- Disaster recovery and business continuity procedures.

5.3.4 Retraining Frequency and Requirements

Individuals responsible for performing DOE CA trusted roles shall be aware of changes in the relevant CA's 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 DOE PKI software or hardware upgrade, changes in security systems, and relocation of equipment.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

The DOE-PMA shall take actions involving any DOE CA or its repository not authorized in this CP, the relevant DOE CPS(s), or other procedures published by the DOE Operational Authority as per section 1.3.1.3.

5.3.7 Contracting Personnel Requirements

Contractor personnel employed by DOE sites to perform functions pertaining to a DOE CA shall be subject to the same criteria as DOE site employees. PKI vendors who provide any services shall establish procedures to ensure that any subcontractors perform in accordance with the DOE CPS and this policy.

5.3.8 Documentation Supplied to Personnel

DOE CAs shall make available to its RA and DOE-SRAA personnel the certificate policies it supports, relevant parts of the DOE CPS, and any relevant statutes, policies or contracts. Documentation shall be maintained identifying all personnel who fulfill trusted roles in the DOE PKI including sufficient identification information, indication that the individual received training and the level of training completed.

6 TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 DOE PKI and DOE CA Signature Key Pair Generation

Cryptographic keying material for certificates issued by any DOE CA shall be generated in FIPS 140 validated cryptographic modules. For the DOE Principal CA and DOE Site CAs, the modules shall meet or exceed Security Level 3. For the DOE-RAs, the modules shall meet or exceed Security Level 2. All DOE CAs will document the key generation procedure in their CPS and provide auditable evidence, as stipulated in section 4.5, that documented procedures were followed and appropriate role separation was used. An independent third party shall validate this process.

6.1.2 Private Key Delivery to End Entity

CAs and End Entities shall have keys delivered in accordance with the requirements of this CP and the applicable CAs CPS .

6.1.3 Public Key Delivery to Certificate Issuer

Public keys shall be delivered to the certificate issuer in an authenticated manner set forth in the relevant DOE CPS. This is usually via a certificate request message. It may also be accomplished via appropriate non-electronic means. These means may include, but are not limited to, floppy disk (or other storage medium) sent via registered mail or courier, or by delivery of a token to a certificate issuer for local key generation at the point of certificate issuance or request. If off-line means are used, they shall include identity checking as set forth in this DOE CP and shall also ensure that proof of possession of the corresponding private key is accomplished.

6.1.4 DOE CA Certificates and Public Key Availability and Delivery to Principal CAs

All DOE CAs shall post the certificates it issues in the DOE PKI repository. Each DOE CA must ensure the authenticated and integral delivery of the trusted self-signed certificate to all issuers and users.

6.1.5 Key Sizes

All FIPS-approved signature algorithms shall be considered acceptable. If the DOE-PMA determines that the security of a particular algorithm may be compromised, it may require the DOE CAs to revoke the affected certificates.

All certificates issued by medium assurance DOE CAs shall use, at least, 2048 bit Rivest-Shamir-Adleman (RSA) or Digital Signature Algorithm (DSA), or better, with Secure Hash Algorithm version 1 (SHA-1) in accordance with FIPS 186. Use of Secure Sockets Layer (SSL)

or another protocol providing similar security shall require, at a minimum, triple-DES (Data Encryption Standard) or equivalent (such as Advanced Encryption Standard [AES]) for the symmetric key, and 2048 bit RSA or equivalent for the asymmetric keys. The specific methods used will be specified in the relevant CA's CPS.

6.1.6 Public Key Parameters Generation

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

6.1.7 Parameter Quality Checking

Parameter quality checking (including primarily testing for prime numbers) shall be performed in accordance with FIPS 186 or a more stringent test if specified by the DOE-PMA.

6.1.8 Hardware/Software End Entity Key Generation

For End Entities, software or hardware shall be used to generate pseudo-random numbers, key pairs and symmetric keys. Any pseudo-random numbers used for key generation material shall A certificate used for encryption and authentication may not be used for non-repudiation. CAs are limited to signing of certificates and CRLs and may not use their certificates for other purposes. The use of a specific key is determined by the key usage extension in the X.509 certificate. End Entities may use the same certificate for signing and authentication.

be generated by a FIPS approved method.

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

6.2 Private Key Protection

6.2.1 Standards for Cryptographic Modules

The relevant standard for cryptographic modules is Security Requirements for Cryptographic Modules, FIPS 140-1 or 140-2. Cryptographic modules shall be validated to the FIPS 140-1 or 140-2 level identified in this section.

Subscribers that have keys granted at medium assurance shall use cryptographic modules, which meet at least the criteria specified in FIPS 140-1 or 140-2 for Level 1 (hardware or software).

All DOE CA shall use hardware cryptographic modules for CA key generation and protection, validated at FIPS 140-1 or 140-2 Level 3 or above.

The DOE-SRAA shall use software or hardware cryptographic modules for key generation and protection, validated at FIPS 140-1 or 140-2 Level 2 or above.

6.2.2 DOE CA Private Key Multi-person Control

Enabling any DOE CA private signing key for use shall require action by multiple persons as set for in Section 5.2.3 of this CP.

6.2.3 Key Escrow

Under no circumstances shall a party other than the Subscriber hold in trust a key used for non-repudiation purposes. Third-party escrow services are not authorized by this policy. DOE CAs may escrow end entity keys that are used for purposes other than digital signatures or non-repudiation.

6.2.4 Private Key Backup

6.2.4.1 Backup of DOE CA Private Signature Key

If DOE CA private signature keys are backed up, they shall be backed up under the same multi person control as the original signature key. Such backup shall create only a single copy of the signature key at the DOE CA location; a second copy may be kept at the DOE CA backup location. Procedures for this process will be included in the relevant CPS.

6.2.4.2 Backup of End Entity Private Signature Key

End Entity's private signature keys may be backed up, but must be held in the End Entity's sole control at all times or as stipulated by the DOE-PMA.

6.2.5 Private Key Archival

Private signature keys shall not be archived, escrowed, or copied except as explicitly allowed in section 6.2.5.

6.2.6 Private Key Entry into Cryptographic Modules

Private keys are to be generated by and remain in a cryptographic module. In the event that a private key is to be transported from one cryptographic module to another, benign techniques must be used. The private key must be encrypted during transport; private keys must never exist in plaintext form outside the cryptographic token boundary.

6.2.7 Method of Activating Private Keys

The End Entity must be authenticated to the cryptographic module before the activation of any private key(s). Approved means of authentication include pass-phrases, PINs, smart cards, biometrics or other devices/technologies approved by the PMA. Entry of activation data shall be protected from disclosure (i.e., the data should not be displayed while it is entered).

6.2.8 Methods of Deactivating Private Keys

If software cryptographic modules are used to store End Entity private keys, they shall not be left unattended when activated or otherwise available to unauthorized access. After use, the cryptographic module shall be deactivated, e.g., via a manual logout procedure, or automatically after a period of inactivity as defined in the applicable CPS.

If hardware cryptographic modules are used to store End Entity private keys, they shall not be left unattended when activated or otherwise available to unauthorized access. After use, the cryptographic module shall be deactivated, e.g., via a manual logout procedure, or automatically after a period of inactivity as defined in the applicable CPS. When End Entity hardware cryptographic modules are not in use, they will be in sole control of the owner at all times.

Regarding all DOE CAs, hardware cryptographic modules shall be removed and stored in a container commensurate with the medium assurance level when not in use.

6.2.9 Method of Destroying End Entity's Private Signature Keys

End Entity private signature keys shall be destroyed when they are no longer needed, or when the certificates to which they correspond expire or are revoked.

For software cryptographic modules, this can be overwriting the data in a manner consistent with NIST, DOD or NSA approved techniques. For hardware cryptographic modules, a certified refresh by the vendor is required. Physical destruction of hardware shall not be required.

6.3 Good practices regarding Key-Pair Management

All DOE CAs shall issue dual key pair certificates. One key pair used for digital signature and one pair for encryption.

An End Entity's key-pair that is used for digital signatures shall never be escrowed, archived or backed up (except as explicitly allowed in section 6.2.4.2). For information that is encrypted, the End Entity shall use his or her private decryption (confidentiality) key to decrypt the information. If that private key is lost or destroyed, or if the End Entity departs the agency without relinquishing the private key, or acts maliciously, there is no way to decrypt the information. Thus, for business continuity reasons, the DOE Site CAs shall escrow, backup or archive private keys used for decrypting files and e-mails, while not escrowing, backing up or archiving key-pairs used for authentication. This means that two separate key pairs must be employed.

6.3.1 Public Key Archival

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

6.3.2 Usage Periods for the DOE Site CA Public and Private Keys

DOE Site CA private signing keys will be used to sign End Entity certificates not for more than one-half of the certificate lifetime. DOE Site CA certificate lifetime will be valid for not more than 6 years.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

A pass phrase or personal identification number (PIN) shall be used to protect access to use of private key. The activation data may be user selected but should consist of at least 8 characters containing both alphabetical and numeric characters. Automated activation data shall be generated in conformance with [FIPS112].

If the activation data must be transmitted, it shall be via a channel of appropriate protection, and distinct in time and place from the associated cryptographic module. If this is not done by hand, the user should be advised of the shipping date, method of shipping, and expected delivery date of any activation data. Users should receive (and acknowledge) a user advisory statement to help to understand responsibilities in the use and control of the cryptographic module.

6.4.2 Activation Data Protection

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

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

The following computer security functions shall be provided by the operating system, or through a combination of operating system, software, and physical safeguards. DOE CA's and their ancillary parts shall include the following functionality:

- Require authenticated logins,
- Provide Discretionary Access Control,
- Provide a security audit capability,
- Restrict access control to DOE CA services and PKI roles,
- Enforce separation of duties for PKI roles,
- Require authentication of PKI roles and associated identities,

- Prohibit object re-use or require separation for DOE CA system random access memory,
- Require use of cryptography for session communication,
- Require use of cryptography for database security,
- Archive DOE CA history and audit data,
- Require self-test security related DOE CA services,
- Require a trusted path for identification of PKI roles and associated identities,
- Enforce domain integrity boundaries for security critical processes, and;
- Require a recovery mechanism for keys and the DOE PKI system.

When DOE CA equipment is hosted on evaluated platforms in support of computer security assurance requirements then the system (hardware, software, operating system) shall, when possible, operate in an evaluated configuration. At a minimum, such platforms shall use the same version of the computer operating system as received the evaluation rating, and shall meet FIPS specifications as delineated in this section. The DOE-PMA may grant an exception if needed to permit secure, reliable operation.

6.5.2 Computer Security Rating

No stipulation.

6.6 Life-Cycle Technical Controls

6.6.1 System Development Controls

The System Development Controls for DOE CAs (impliedly DOE-RAs) are as follows:

- Hardware and software procured to operate DOE CAs shall be purchased 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),
- Hardware and software developed for DOE CAs shall be developed in a controlled environment, and the development process shall be defined and documented,
- All hardware must be shipped or delivered via controlled methods that provide a continuous chain of accountability, from the purchase location to the DOE CA physical location,
- DOE CA hardware and software shall be dedicated to performing one task: DOE CA operations. There shall be no other applications, hardware devices, network connections, or component software, which are not part of DOE CA operation,
- Proper care shall be taken to prevent malicious software from being loaded onto DOE CA equipment. Only applications required to perform the operation of the DOE CA shall be

obtained from sources authorized by local policy. DOE-RA hardware and software shall be scanned for malicious code on first use and periodically afterward, 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.

DOE CA hardware and software shall be dedicated to performing one task: DOE CA operations. There shall be no other applications, hardware devices, network connections, or component software, which are not part of DOE CA operation. The DOE-RA hardware can be used for other functions directly related to authentication and systems account management but must not access unsecured servers (e.g. web pages) outside the local site firewall. The CPS must specify control, access, and security practices to be used to protect the RA from malicious or accidental intrusion. All of the obligations in the CP in sections 2.1.1 and 2.1.2 must be stipulated.

6.6.2 Security Management Controls

The configuration of DOE CA systems as well as any modifications and upgrades shall be documented and controlled. There shall be a mechanism for detecting unauthorized modification to DOE CA software or configuration. A formal configuration management methodology shall be used for installation and ongoing maintenance of DOE CA systems. DOE 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.

6.6.3 Life Cycle Security Ratings

No stipulation.

6.7 Network Security Controls

A network guard, firewall or filtering router must protect network access to DOE CA equipment. The network guard, firewall or filtering router shall limit services allowed to and from the DOE CA equipment to those required to perform DOE CAA functions. Protection of DOE CA equipment shall be provided against known network attacks. All unused network ports and services shall be turned off. Any network software present on the DOE CA equipment shall be necessary to the functioning of the DOE CA application. DOE Principal CA equipment shall be stand-alone (off-line) configurations. Any boundary control devices used to protect the network on which PKI equipment is hosted shall deny all but the necessary services to the PKI equipment even if those services are enabled for other devices on the network. The DOE CPS shall define the network protocols and mechanisms required for the operation of the relevant DOE CA and any Border Directory or repository.

7 CERTIFICATE AND CRL PROFILES

7.1 Certificate Profile

The Federal PKI Technical Working Group defines the certificate profile for us in the Federal Government PKI community. DOE will use the *Federal Public Key Infrastructure (PKI) X.509 Certificate and CRL Extensions Profile*, dated 2 July 2002, as a baseline for its certificate profile. Each CA's CPS must identify any discrepancies between its own certificate profile and the FPKI profile.

7.1.1 Version Numbers

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

7.1.2 Certificate Extensions

Rules for the inclusion, assignment of value, and processing of extensions are defined in profiles. Certificate extensions used by DOE CAs shall conform to the Federal certificate profile established by NIST. Critical private extensions shall be interoperable in their intended community of use.

7.1.3 Algorithm Object Identifiers

Certificates issued under the DOE CP shall use the following OIDs for signatures:

Table 7.1.3-1 Algorithm 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}

Certificates under the DOE CP will use the following OIDs for identifying the algorithm for which the subject key was generated:

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-keyExchangeAlgorithm	{iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) id-mod(0) id-mod-kea-profile-88(7)}

Keys generated for use with RSA shall be signed using sha-1WithRSAEncryption.

7.1.4 Name Forms

Where required as set forth above, the subject and issuer fields of the base certificate shall be populated with an X.500 Distinguished Name, with the attribute type as further constrained by RFC 2459.

7.1.5 Name Constraints

DOE CAs shall assert name constraints in certificates issued as required to comply with the FBCA and PKIX standards.

7.1.6 Certificate Policy Object Identifier

Certificates issued under this policy shall assert the DOE CP policy OID as defined in section 1.2.

7.1.7 Usage of Policy Constraints Extension

No stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

Certificates issued under the DOE CP shall not contain policy qualifiers.

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

Processing semantics for the critical certificate policy extension used by all DOE CAs shall conform to the Federal certificate profile issued by NIST.

7.2 CRL Profile

7.2.1 Version Numbers

All DOE CAs shall issue X.509 version two (2) CRLs.

7.2.2 CRL Entry Extensions

CRL Entry extensions will conform to the Federal PKI Certificate profiles which can be found at http://csrc.ncsl.nist.gov/pki/FPKI7-10.doc and will be specified in Principal and Site CA CPS(s).

8 SPECIFICATION ADMINISTRATION

8.1 Specification Change Procedures

The DOE-PMA shall review this CP at least once every year. The DOE-PMA shall maintain and publish a Certificate Policy Plan that describes anticipated changes to this CP. Errors, updates, or suggested changes to this CP shall be communicated to every End Entity. Such communication must include a description of the change, a change justification, and contact information for the person requesting the change.

All policy changes under consideration by the DOE-PMA shall be disseminated to interested parties. All interested parties shall provide their comments to the DOE-PMA in a fashion to be prescribed by the DOE-PMA.

8.2 Publication and Notification Policies

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

8.3 DOE CPS Approval Procedures

The term CPS is defined in the Internet X.509 Public Key Infrastructure Certificate Policy and Certificate Practices Framework as: "A statement of the practices, which a Certification or Certification Authority employs in issuing certificates." It is a comprehensive description of such details as the precise implementation of service offerings and detailed procedures of certificate life-cycle management. The relationship between the DOE CP and DOE CPS(s) is described in section 1.1.2. The DOE CPS, which is contained in a separate document published by each Site and approved by the DOE-PMA, specifies how this CP is implemented to ensure compliance.

8.4 Waivers

The DOE-PMA will develop and publish procedures pertaining to this area. Waivers will be valid for up to one year, and may be renewed once. After the two-year maximum period, a change to this policy will be required.

9 REFERENCES

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

ABA American Bar Association, Section of Science & Technology, *Digital Signature Guidelines,* 1996, (http://www.abanet.org/scitech/ec/isc/dsg.pdf)

American Bar Association, Section of Science & Technology, *PKI Assessment Guidelines* (http://www.abanet.org/scitech/ec/isc/pagv30.pdf

TCSEC U.S. Department of Defense, *Department of Defense Trusted Computer System Evaluation Criteria*, DOD 5200.28-STD http://www.disa.mil/MLS/info/orange/intro.html; http://csrc.nist.gov/secpubs/rainbow/std001.txt.

TSDM U.S. Department of Defense, "Trusted Software Methodology," Volume 1, SDI-S-SD-91-000007, Department of Defense, Strategic Defense Initiative Organization, 17 June 1992.

FIPS 112 Password Usage, 1985-05-30, http://csrs.nist.gov/fips/.

FIPS 140-1 Security Requirements for Cryptographic Modules, 1994-01, http://csrs.nist.gov/fips/fips1401.htm.

FIPS 140-2 Security Requirements for Cryptographic Modules, 2001-05 http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf.

FIPS 180-1 Secure Hash Standard, 1995-04 http://csrc.nist.gov/publications/fips/fips180-1/fip180-1.pdf.

FIPS 186 Digital Signature Standard, 1994-05-19, http://csrs.nist.gov/fips/fips186.pdf.

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

FPKI-E Federal PKI Version 1 Technical Specifications: Part E-X.509 Certificate and CRL Extensions Profile, 7 July 1997, http://csrs.nist.gov/pki/FPKI7-10.DOC.

ISO9594-8 Information Technology-Open Systems Interconnection-The Directory: Authentication Framework, 1997, ftp://ftp.bull.com/pub/OSIdirectory/ITU/97x509final.doc.

ITMRA 40 U.S.C. 1452, Information Technology Management Reform Act of 1996, http://www4.law.cornell.edu/uscode/40/1452.html.

NAG69C Information System Security Policy and Certification Practice Statement for Certification Authorities, rev C, November 1999.

NSD42 National Policy for the Security of National Security Telecom and Information Systems, 5 Jul 1990, http://snyside.sunnyside.com/cpsr/privacy/computer_security/nsd_42.txt (redacted version).

NS4005 NSTISSI 4005, Safeguarding COMSEC Facilities and Material, August 1997.

NS4009 NSTISSI 4009, National Information Systems Security Glossary, January 1999.

PKCS#12 Personal Information Exchange Syntax Standard, April 1997, http://www.rsa.com/rsalabs/pubs/PKCS/html/pkcs-12.html.

RFC 2510 Certificate Management Protocol, Adams and Farrell, March 1999

RFC 2527 Certificate Policy and Certificate Practices Framework, Chokhani and Ford, March 1999.]

RFC 2459 Internet X.509 Public Key Infrastructure Certificate and CRL Profile, Housley, Polk, Ford, and Solo, January, 1999

10 ACRONYMS AND ABBREVIATIONS

AES	Advanced Encryption Standard
ARL	Authority Revocation List
CA	Certification Authority
CAA	Certification Authority Administrator
CAW	Certification Authority Workstation
COMSEC	Communications Security
CP	Certificate Policy
CPS	Certification Practices Statement
CRL	Certificate Revocation List
DN	Distinguished Name
DOE	US Department of Energy
DOE-PMA	Department of Energy Policy Management Authority
DOE PKI	Public Key Infrastructure operated by and maintained for the Department of Energy
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
FIPS	Federal Information Processing Standard
FIPS PUB	(US) Federal Information Processing Standard Publication
FPKIPA	Federal PKI Policy Authority
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISO	International Organization for Standardization
ISSO	Information Systems Security Officer
ITC	Information Technology Center
ITU	International Telecommunications Union
MOA	Memorandum of Agreement

NIST	National Institute of Standards and Technology
OID	Object Identifier
PCA	Principal Certification Authority
PIN	Personal Identification Number
PKCS	Public Key Certificate Standard
PKI	Public Key Infrastructure
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure - X.509 (IETF Working Group)
PMA	Policy Management Authority
RA	Registration Authority
RAA	Registration Authority Administrator
RFC	Request For Comments
RSA	Rivest-Shamir-Adelman encryption algorithm
S/MIME	Secure Multipurpose Internet Mail Extension
SA	System Administrator
SHA-1	Secure Hash Algorithm, Version 1
SSL	Secure Sockets Layer
TBD	To be determined
TCSEC	Trusted Computer System Evaluation Criteria
U.S.C.	United States Code
UCNI	Unclassified Controlled Nuclear Information
UPS	Uninterrupted Power Supply
URL	Uniform Resource Locator

11 GLOSSARY

Access	Ability to make use of any information system (IS) resource. [NS4009]
Access Control	Process of granting access to information system resources only to authorized users, programs, processes, or other systems. [NS4009]
Accreditation	Formal declaration by a Designated Approving Authority that an Information System is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. [NS4009]
Activation data	Data (other than keys) required for operating hardware or software cryptographic modules. Examples include personal identification numbers (PINs), passwords, and pass phrases.
Agency	Any peer element of the Department of Energy, or independent organizational entity that is statutorily or constitutionally recognized as being part of the Department.
Agency CA	A CA that acts on behalf of an Agency, and is under the operational control of an Agency.
Applicant	The End Entity 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.
Attribute Authority	An entity, recognized by the DOE-PMA or comparable Agency body as having the authority to verify the association of attributes to an identity.
Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures. [NS4009]
Audit Data	Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event. [NS4009, "audit trail"]
Authenticate	To confirm the identity of an entity when that identity is presented.
Authentication	The process of establishing identity based on the possession of a trusted credential.
Authority Revocation List (ARL)	A list of cross-certificates previously issued by the subject CA that have been subsequently compromised or otherwise

	invalidated.
Backup	Copy of files and programs made to facilitate recovery if necessary. [NS4009]
Benign	A method that does not allow for corruption or misuse.
Binding	Process of associating two related elements of information. [NS4009]
CA Facility	The collection of equipment, personnel, procedures and structures that are used by a Certification Authority to perform certificate issuance and revocation. May include collection of equipment, personnel, procedures and structures that are used to register applicants for certificate issuance.
Certificate	A digital representation of information which at least (1) identifies the Certification Authority issuing it, (2) names or identifies its End Entity, (3) contains the End Entity's public key, (4) identifies its operational period, and (5) is digitally signed by the Certification Authority issuing it. As used in this CP, the term "Certificate" refers to certificates that expressly reference the OID of this CP in the "Certificate Policies" field of an X.509 v.3 certificate.
Certificate	A digital representation of information which at least (1) identifies the Certification Authority issuing it, (2) names or identifies it's End Entity, (3) contains the End Entity's public key, (4) identifies it's operational period, and (5) is digitally signed by the Certification Authority issuing it.
Certificate Management Authority (CMA)	A Certification Authority or a Registration Authority.
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.
Certificate Revocation List (CRL)	A list maintained by a Certification Authority of the certificates which it has issued that are revoked prior to the stated expiration date.
Certificate Status Authority	A trusted entity that provides on-line verification to a relying party of a subject certificate's trustworthiness, and may also

	provide additional attribute information for the subject certificate.
Certificate-Related Information	Information, such as an End Entity's postal address, that is not included in a certificate, but that may be used by a CA in certificate management.
Certification Authority	Certification Authorities are those entities that are comprised of CAs. Examples of certification authorities are the FBCA (see below) or Identrus. But, in each case these certification authorities are made of a collection of Certificate Authorities (CAs).
Certification Authority (CA)	The CA is a central authority in a PKI that issues, manages, and revokes digital certificates; the CA is an entity, a piece of hardware running a vendor's piece of software.
Certification Authority (CA)	An entity responsible for issuing, signing (certifying), and managing public key certificates (sometimes referred to as a Certification Authority.)
Certification Authority Software	The cryptographic software required managing the certificates of End Entities.
Certification Authority workstation (CAW)	The computer system or systems that process Certification Authority software and/or have access to the CA private keys, End Entity private keys, or End Entity public keys prior to certification.
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).
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.
Common Criteria	A set of internationally accepted semantic tools and constructs for describing the security needs of customers and the security attributes of products.
Complying CA	A CA operating in compliance with this Certificate Policy and other applicable Federal and DOE policies and regulations.
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.
Confidentiality	Assurance that information is not disclosed to unauthorized entities or processes.
Cross-Certificate	A certificate used to establish a trust relationship between two

	Certification Authorities.
Cryptographic Module	The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module. [FIPS1401]
Cryptoperiod	Time span during which each key setting remains in effect. [NS4009]
Data Integrity	Assurance that the data are unchanged from creation to reception.
Decryption private key	A private key used to decrypt data or session keys encrypted by the corresponding public key.
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.
DOE community	The US Department of Energy (DOE), or any person or organization operating under the authority and direction of the DOE, either directly or through a contractual relationship.
DOE Operational Authority	The DOE Operational Authority is the organization that manages and operates DOE CAs. It is comprised of executives and/or decision makers.
DOE PKI	This term refers to the aggregation of all Certificate Authorities (CAs) that assert this policy, and the other PKI components (Registration Authorities, Directories, Certificate Policies and Certificate Practice Statements) that are used to provide digital signature and encryption key certificates to DOE Subscribers.
DOE Site CA	Site CAs are the CAs which are certified by the Principal CA and issue certificates to individual in the DOE.
DOE-PMA	The DOE-PMA is responsible for setting, implementing, and administering policy decisions regarding interagency PKI interoperability that uses the DOE PKI. The DOE dutifully designated individual (or group) will fulfill this role.
Domain (of a CA)	The scope of authority of a CA, generally limited to RAs and end entities registered with or certified by the CA.
Dual Use Certificate	A certificate that is intended for use with both digital signature and data encryption services.

Duration	A field within a certificate that is composed of two subfields; "date of issue" and "date of next issue".
E-commerce	The use of network technology (especially the internet) to buy or sell goods and services.
Employee	Any person employed by an Agency as defined above.
Encryption certificate	A certificate containing and conveying a public key used to encrypt electronic messages, files, documents, data transmissions, etc., or to establish a session key for those purposes.
End Entity (EE)	A person or a computer system that is a subject or user of a certificate, but is not a CA or RA. An End Entity is a End Entity, a relying party, or both.
Federal PKI PA	The Federal PKI Policy Authority is the entity responsible for policy mapping and approval of policies for cross-certification with the Federal Bridge CA.
Firewall	Gateway that limits access between networks in accordance with local security policy. [NS4009]
Government information	Defined by Office of Management and Budget (OMB) Circular A-130 as all information created, collected, processed, disseminated, or disposed of by or for the Federal government.
Inside Threat	An entity with authorized access that has the potential to harm an information system through destruction, disclosure, modification of data, and/or denial of service.
Integrity	Protection against unauthorized modification or destruction of information. [NS4009]. 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 End Entity and other pertinent information pursuant to an escrow agreement or similar contract binding upon the End Entity, the terms of which require one or more agents to hold the End Entity's private key for the benefit of the End Entity, an employer, or other party, upon provisions set forth in the agreement. [adapted from ABADSG, "Commercial key escrow service"]
Key Exchange	The process of exchanging public keys in order to establish protected communication.
Key Generation Material	Random numbers, pseudo-random numbers, and cryptographic

	parameters used in generating cryptographic keys.
Key materials	A tangible representation of a key. Examples include a key stored in computer memory, computer disk, smart card, or other key carrier.
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 one key, it is computationally infeasible to discover the other key.
Local Registration Authority (LRA)	A Registration Authority with responsibility for a specific community.
Memorandum of Agreement (MOA)	Agreement between the DOE-PMA and an Agency allowing interoperability between the DOE Principal CA and the DOE Site CAs.
Mission Support Information	Information that is important to the support of deployed and contingency forces.
Mutual Authentication	Occurs when parties at both ends of a communication activity authenticate each other (see authentication).
Naming Authority	An organizational entity responsible for assigning distinguished names (DNs) and for assuring that each DN is meaningful and unique within its domain.
National Security System	Any telecommunications or information system operated by the United States Government, the function, operation, or use of which involves intelligence activities; involves cryptographic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions, but does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). [ITMRA]
Non-Repudiation	Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data. [NS4009] 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 with an internationally recognized standards organization. The unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class. In the federal government PKI they are used to uniquely identify each of the four policies and cryptographic algorithms supported.

Out-of-Band	Communication between parties utilizing a means or method that differs from the current method of communication (e.g., one party uses U.S. Postal Service mail to communicate with another party where current communication is occurring online).
Outside Threat	An unauthorized entity from outside the domain perimeter that has the potential to harm an Information System through destruction, disclosure, modification of data, and/or denial of service.
Physically Isolated Network	A network that is not connected to entities or systems outside a physically controlled space.
PKI	See Public Key Infrastructure.
PKI Sponsor	Fills the role of a End Entity for non-human system components that are named as public key certificate subjects, and is responsible for meeting the obligations of End Entities as defined throughout this CP.
Policy Certification Authority (PCA)	A DOE entity that formulates policy, and oversees the operation of public key infrastructures within the DOE, as specified in the DOE Telecommunications Manual, Chapter 9, "*Policy for the Use of Public Key Cryptography and Key Management.*"
Policy Management Authority (PMA)	A DOE committee with representatives from organizations operating CAs within the DOE, as specified in the DOE Telecommunications Manual, Chapter 9, "*Policy for the Use of Public Key Cryptography and Key Management.*"
Principal CA (DOE Principal CA)	The Principal CA is the CA that certifies all individual Site CAs (or DOE Site CAs). This CA performs cross-certification with the Federal Bridge CA. The Principal CA does not issue certificates to subscribers.
Privacy	Restricting access to End Entity or relying party information in accordance with Federal law and agency 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 private or sensitive 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 private or sensitive information. In both cases, this key is made publicly available normally in the form of a digital certificate.
Public key algorithm	A cryptographic algorithm in which the encryption and decryption functions are divided between a pair of mathematically related keys. In some common public key algorithms (e.g., RSA[3]), the

[3] The public-private key algorithm developed by Rivest, Shamir, and Adelman, currently owned by RSA Data Security, Inc.

	encryption/decryption functions are reciprocal, i.e., either key of the pair can be used to encrypt or decrypt, with the other key able to decrypt or encrypt respectively.
Public key certificate	The public key portion of a public-private key pair, that has been digitally signed by a CA, thereby certifying the validity and data integrity of the public key contained in the certificate, in accordance with the applicable Certificate Policy.
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)	The hardware and software that is used to communicate with DOE CAs for certificate requests.
Registration Authority Administrator (RAA)	An entity that is responsible for authentication of certificate subjects, but that does not sign or issue certificates (i.e., a Registration Authority Administrator is delegated certain tasks on behalf of an authorized DOE CA). The RAA uses the RA equipment to perform the registration functions.
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 on the new public key.
Relying Party	A person or Agency who has received information that includes a certificate and a digital signature verifiable with reference to a public key listed in the certificate, and is in a position to rely on them.
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).
Responsible Individual	A trustworthy person designated by a sponsoring organization to authenticate individual applicants seeking certificates on the basis of their affiliation with the Sponsor.
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.
Risk Tolerance	The level of risk an entity is willing to assume in order to achieve a potential desired result.
Server	A system entity that provides a service in response to requests from clients.

Signature Certificate	A public key certificate that contains a public key intended for verifying digital signatures rather than encrypting data or performing any other cryptographic functions.
Signature verification certificate	A certificate containing and conveying a public key used to verify a digital signature created by the associated signing private key. Also called a verification certificate.
Signing private key	A private key used to create digital signatures.
Sponsor	A person or organization with which the End Entity is affiliated (e.g., as an employee, user of service, or customer).
Subscriber	A human End Entity that has been issued a certificate by a DOE CA in compliance with this policy, and whose public key and distinguished name are certified in the certificate.
Symmetric algorithm	An cryptographic algorithm in which data is encrypted and decrypted using the same key.
System Equipment Configuration	A comprehensive accounting of all system hardware and software types and settings.
Technical non-repudiation	The contribution public key mechanisms to the provision of technical evidence supporting a non-repudiation security service.
Threat	Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service. [NS4009]
Trust List	Collection of trusted certificates used by relying parties to authenticate other certificates.
Trusted Agent	Entity authorized to act as a representative of a Registration Authority in confirming End Entity identification during the registration process. Trusted Agents do not have automated interfaces with Certification Authorities. Further, Trusted Agents have a trust relationship with the RA that is stronger than that of a Designated Representative.
Trusted Certificate	A certificate that is trusted by the relying party on the basis of protected, authenticated delivery. The public keys included in trusted certificates are used to start certification paths. Also known as a "trust anchor".
Trusted Software Development Methodology (TDSM)	Trusted Software Development Methodology (TDSM) was developed to define trust levels (1-5) based upon 25 trust principals. TSDM has much in common with the Software Engineering Institute (SEI) Capability Maturity Model (CMM) for software development and is focused on the software development process.
Trusted Timestamp	A digitally signed assertion by a trusted authority that a specific digital object existed at a particular time.

Trustworthy System	Computer hardware, software and procedures that: (1) are reasonably protected from intrusion and misuse; (2) provide a reasonable level of availability, reliability, and correct operation; (3) are reasonably suited to performing their intended functions; and (4) adhere to generally accepted security procedures.
Two-Person Control	Continuous surveillance and control of positive control material at all times by a minimum of two authorized individuals, each capable of detecting incorrect and/or unauthorized procedures with respect to the task being performed, and each familiar with established security and safety requirements. [NS4009]
Update (a certificate)	The act or process by which data items are 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. [FIPS1401]