Federal Public Key Infrastructure (PKI) Technical Specifications (Version 1) Part B: Technical Security Policy

Table of Contents

1. Introduction and Background 1

2. Assumptions 1

3. Federal PKI Component Responsibilities 2
   3.1 Certificate Authorities (CA) 2
      3.1.1 Root CA 3
      3.1.2 Leaf CAs 3
   3.2 Organizational Registration Authorities (ORA) 3
   3.3 Additional Supporting Elements 4
      3.3.1 Policy Approval Authority (PAA) 4
      3.3.2 Directory Service (DS) 4
      3.3.3 Computer Security Objects Register (CSOR) 5

4. CA Operational Policy 5
   4.1 Uniform Operational Requirements 6
   4.2 Requirements for Low Assurance CAs 7
   4.3 Requirements for Medium Assurance CAs 7
   4.4 Requirements for High Assurance CAs 8

5. Certificate Issuance Policies 9
   5.1 CA Certificates 9
   5.2 ORA Certificates. 9
   5.3 Low Assurance User Certificate 10
   5.4 Medium Assurance User Certificate 10
   5.5 High Assurance User Certificate 11

6. Federal Assurance Levels 12

7. Federal PKI Management 13

8. Records Keeping 13

9. CA Failure and Compromise Recovery 14
   9.1 Backup Policy 14
   9.2 Notification Procedures 14

9.3 Initialization Procedures 14

10. Certificate Revocation 14

11. Cross Certification Guidelines 15

12. Additional Services 16
12.1 Confidentiality Key Backup 16
12.2 Secure Session Key Establishment 16

13. References 16

Annex 1 - Quality Tests for DSA Key Material 18

Annex 2 - Security Policy Object Definition 19

Federal Public Key Infrastructure (PKI) Technical Specifications (Version 1) Part B: Technical Security Policy

1. Introduction and Background

This document provides a technical framework for the enforcement of a security policy for the Federal Public Key Infrastructure (PKI), establishes basic operational procedures, and details policy constraints that guide its design and development. The Federal PKI supports end user authentication, data integrity, data confidentiality, and source non-repudiation. The Federal PKI is also responsible for recording its transactions to allow the verification of the validity of user transactions authenticated or protected using the public key certificates it creates and maintains.

This document covers technical policy issues related to the generation, deactivation, and dissemination of public key certificates; the establishment of session cryptographic material; the organization and responsibilities of the certification authorities and the users of the Federal PKI; records keeping requirements; and the relationships between the Federal PKI and other certification infrastructures.

This document defines the technical controls and requirements associated with Certificate Authority (CA) certificates, Organization Registration Authority (ORA) certificates, Cross Certificates, and Federal PKI User certificates. It identifies three types of User certificates supporting increasingly stringent security policies. The policies supported differ in their certificate owner identification and authentication requirements and the level of protection afforded by the CAs involved in the creation of the certificates. Furthermore, the document outlines how support for other security policies may be provided.

2. Assumptions

The Federal PKI provides public key certificate management and related security services that will help U. S. Government agencies secure electronic transactions, prove the authenticity of electronic documents, and maintain temporal records of the occurrence of certain events. The target consumers of Federal PKI services are employees of the Federal, State, and Local Governments, Government trading partners, benefit recipients, tax payers, citizens, and subscribers of other infrastructures. This document adopts some of the nomenclature defined in the *Public Key Infrastructure Study* [11] as interpreted and presented in the *Federal PKI Concept of Operations* [2] (CONOPS).

The Federal PKI is organized as a hierarchy for practical and administrative reasons. At the same time, and through the use of cross certificates, it can be traversed as a network of systems. As

indicated in the CONOPS [2], trust is delegated hierarchically and most cross certificates are required to preserve that delegation. The use of special cross certificates can override restrictions imposed on trust and naming space, but their use is limited to "leaf" CAs to limit the circumvention of restrictions to only affect the users of the cross certified CAs.

CAs and ORAs within Federal PKI shall sign certificates and Certificate Revocation Lists (CRLs) using the Digital Signature Algorithm (DSA) specified in FIPS PUB 186 - *Digital Signature Standard* (DSS) [7]. Users of the Federal PKI will create their own signature key pairs and submit the public key to an ORA function who will verify the user's identity and generate a certificate request. The ORA function (i.e., vouching for the identity of the user) is a necessary function and will be present even if it is performed by the same system implementing the CA. The ORA function will also verify that the user requesting certification is in possession of the private keys associated with the public keys presented for certification. Separate certificates will be created for signature public keys and for keys used to provide data confidentiality or to establish security associations providing data confidentiality. Individual agency systems may also generate attribute certificates that are associated with certain signature certificates. Although attribute certificates may be stored under a user's distinguished name in a directory, they are not created or maintained by the Federal PKI.

3. Federal PKI Component Responsibilities

The main components of the Federal PKI are Certificate Authorities (CAs) and Organization Registration Authorities (ORAs). In addition, the Federal PKI relies on the existence of a Directory Service (DS), a Policy Approving Authority (PAA), a PKI Transaction Archive, and the Computer Security Objects Register (CSOR). The CONOPS [2] identifies other peripheral components that support value-added services but are not essential to the Federal PKI.

3.1 Certificate Authorities (CA)

CAs generate, revoke, publish, and archive certificates. They may also impose name space and policy restrictions on its subordinate CAs. All CAs shall either operate, or be associated with, a directory server. They shall also have access to an off-line archive where a log of all transactions are recorded. Every CA operates under one explicitly defined CA Operational Policy, but it may issue certificates under multiple Certificate Issuance Policies. This document defines basic CA Operational Policies (*Section 4*) and Certificate Issuance Policies (*Section 5*) that meet uniform assurance levels for the Federal PKI.

The PAA (*Section 3.3.1*) evaluates CA operational procedures against those basic operational policies to assess the Federal Assurance Levels the CA may include in the certificates it issues. The PAA also takes in consideration the Certificate Issuance Policies of the CA when granting authorization to issue certificates identified with Federal Assurance Levels identifiers. If a Federal

Assurance Level identifier is not included in a certificate, the specific Certificate Issuance Policy under which it was issued shall be identified.

The CAs shall use X.500 name subordination to ensure that each distinguished name is unique. A common naming space may be shared by more than one CA if they coordinate name assignment in a way that preserves the uniqueness of the all names. Distinguished names contain meaningful alphanumeric strings that accurately identify certificate holders.

3.1.1 Root CA

Although the use of cross certificates allows the Federal PKI to be seen as a network of CA's joined through bilateral trust relationships, it is organized as a hierarchy that roughly follows that of the different departments and agencies of the Federal Government. That hierarchy delineates trust delegation within the Infrastructure. Trust and name space restriction imposed by the hierarchy shall be preserved by all Federal PKI CAs, with the possible exception of Leaf CAs (*Section 3.1.2*). The first CA in the Federal PKI hierarchy is known as the Root CA. All trust in the Federal PKI propagates from this CA.

The Root CA may generate and sign its own certificate, its public key is transmitted to its subordinates when requesting initial certification. The Root CA is associated with the PAA (*Section 3.3.1*), which authorizes the use of the Federal Assurance Levels and oversees the operation of the Federal PKI to maintain its integrity and trustworthiness.

3.1.2 Leaf CAs

Leaf CAs are at the bottom of the PKI hierarchy, i.e., they have no subordinate CAs. Like all CAs, these CAs generate user certificates and may cross certify with other CAs. Unlike others, these CAs may cross certify with other Leaf CAs and form special cross certificates that violate the trust and name space restrictions imposed by the hierarchical structure. Since Leaf CAs have no subordinate CAs, these "violations" can only affect the two CAs involved and their users.

3.2 Organizational Registration Authorities (ORA)

The Organizational Registration Authority (ORA) is the function that vouches for the identity of users requesting certification. CA operators and users request initial certification by appearing in person before the ORA for their parent CA and submitting a certificate request consisting of a partially complete certificate signed with the private key for the public key being certified. This self-signing of the certificate request is done to verify that the user is in possession of the complete key pair. The ORA function verifies all the personal and affiliation information on the request and the signature according to the requirements for the type of certificate being requested. Details of the user's identity verification process are discussed in Section 6. After the signature and the user's identity are verified, the ORA signs and sends the certificate request to the CA.

The ORA function may be performed by individuals physically removed from the CA that verify the identity of the user requesting certification and send an electronic certification request on behalf of the user. In that case the certificate request is signed by the ORA. Alternatively, the ORA and CA functions may be collocated. In this case the CA's operator verifies the identity of the user requesting certification prior to issuing the certificate. When these two functions implemented on the same system, the ORA agent verifying the user's identity shall sign a certificate request for accountability purposes but the CA need not verify the signature prior to issuing the certificate.

Each standalone ORA shall perform the following functions:

- Generate its own public-private key pair
- Request the creation of User certificates by the CA
- Verify that the user is in possession of the private key of every public key submitted.
- Deliver user certificates to the owner
- Maintain a list of certificate owners with phone numbers and affiliation information
- Create and maintain system audit logs

ORA operators must be trained on the proper procedures and operation of their system. Security practices such as separation of privilege shall be employed. Operators are instructed and provided with reference material on the proper use and safeguard of key material, audit logs, personal information, archival material, et cetera. Operators are also instructed on the rules for reporting lost or compromised keys.

3.3 Additional Supporting Elements

3.3.1 Policy Approval Authority (PAA)

The Policy Approving Authority (PAA) evaluates CA Operational Policies and Certificate Issuance Policies to assess the overall quality of the certificates issued by each CA. The PAA authorizes Federal PKI CAs to include Federal Assurance Level identifiers in the certificates they issue based on that assessment. The PAA is directly associated with the Root CA, but it delegates oversight responsibilities to subordinate authorities. The PAA and its designated subordinates shall perform annual assessments of every CA in the Federal PKI.

The PAA identifies and delegates responsibilities to subordinate authorities, limits the depth of the PKI hierarchy, approve the use of Federal Assurance Levels, monitors adherence to CA Operational Policies and Certificate Issuance Policies, and may assign name space constraints to CAs and register additional policies for use throughout the Infrastructure.

3.3.2 Directory Service (DS)

The Federal PKI relies on the on-line availability of certificates, certificate revocation lists (CRLs), and other policy information for the validation of public key signatures and establishment of confidentiality-protected communications sessions and messaging applications. The basic mechanism for making that information available is a directory service provided by one or more interconnected directory servers.

The Federal PKI relies on a directory service based on the X.500 Directory [3]. All CAs shall either operate their own directory servers or have access to one. Individual directory servers shall have appropriate visibility and should operate as components of a distributed service. The equipment operating the directory shall provide C2-plus functionality, including mandatory and discretionary access controls. Read access to directory information shall be provided to all users upon request while maintaining strict control on write access to avoid unauthorized modification. All directory information entries shall be signed by the originator using the DSA. At the risk of limiting their ability to communicate securely outside of their communities, certain organizations with special confidentiality requirements may operate directory servers with additional confidentiality and access control limitations.

3.3.3 Computer Security Objects Register (CSOR)

The CSOR administers a segment of the registration authority granted to NIST for the US Federal Government. The CSOR assigns object identifiers (OIDs) to computer security objects with the prefix {joint-iso-ccitt(2) country(16) us(840) gov(101) csor(3) pki(4)} (referred to as csor-pki from now on). Under the PKI OID prefix there will be a branch for CA Operational Policies {csor-pki ca-op-policy(0)}, one for Certificate Issuance Policies {csor-pki cert-issue-policy(1)}, and one for Certificate Policies {csor-pki cert-policy(2)}. Even though they are not policies in the strict sense, the Federal Assurance Levels will be given OIDs under the Certificate Policy branch.

Policies registered in the CSOR are signed by the entity posting the policy. The CSOR does not effect any checks, verifications, or sanctioning of the policies. Only policies and Federal Assurance Levels signed and registered by the PAA are reviewed and sanctioned for use by Federal Government agencies prior to registration. The decision to use any other policy in the generation of certificates, or to accept certificates generated under such policies, is the sole responsibility of the CA. Federal PKI CAs shall obtain the authorization of the PAA prior to including the OID for a Federal Assurance Level in any certificate. The set of policies registered by the PAA is intended to be a minimal non-redundant set that aims to provide uniformity throughout the Federal PKI.

4. CA Operational Policy

The CA Operational Policy explicitly defines the operation of a CA. This includes: backup procedures, record archiving procedures, qualifications of operations personnel, functional roles of CA operators, physical protection afforded to the CA, 140-1 level requirements for CA cryptographic modules, access controls for CA private keys, etc. The CA Operational Policies of CAs in the Federal PKI shall be posted in the NIST Computer Security Objects Register (CSOR) [9].

At a minimum, Federal PKI CAs must comply with the requirements stated in Section 4.2 for low assurance CAs. The uniform requirements in Section 4.1 apply to all three assurance levels.

4.1 Uniform Operational Requirements

All CAs within the Federal PKI sign certificates using the DSA [7]. The DSA parameters *p*, *q*, and *g* used by the CA to sign the certificates it creates may be locally established or assigned by the parent CA. Those parameters are maintained for five years, unless the system is compromised and/or corruption of the locally-maintained certificate-generation data occurs. The parent CA may also request that the parameters used by its subordinates be changed if it is compromised or its database becomes corrupted. The size of the prime modulus *p* shall be 1024 bits for all CAs, ORAs, and users.

Each CA shall perform the following functions:

- Generate its own public-private key pair
- Execute tests for the quality of the public key parameters (i.e., *p*, *q*, and *g*) as identified in Annex 1 (these variables are defined in FIPS PUB 186 [9]).
- Create and deliver subordinate certificates
- Ensure there are no distinguished name collisions within its own name space
- When issuing ORA certificates, subordinate CA certificates, and cross certificates, verify that the CA or ORA requesting the certificate is in possession of the private key for every public key submitted for certification.
- Signing and verifying signatures
- Create, maintain, and distribute CRLs
- Maintain record of certificates it issued
- Create and maintain system audit logs
- Archive certificates and CRLs
- Generate or obtain time stamps
- Revoke certificates

A CA shall generate a certificate for a subordinate CA or a user upon validating the request. Two forms of certification requests shall be supported: initial, whereby the identity of the requestor

must be established in person, at request time; and renewal, whereby the established identity of the requestor is perpetuated with the request. Requests for new user certificates (i.e., not renewals) are always generated by an ORA function that vouches for the identity of the user (*Section 3.2*). The ORA function is responsible for providing and verifying all the required personal and affiliation identification information for the type of certificate being requested.

Upon receipt of a certificate request, a CA shall: (1)verify the signature of the ORA and that the information on the request is accurate, (2) complete the certificate and sign it with its private key, (3) post the new certificate on the DS, and (4) return the new certificate along with it's own certificate. The certificate may be returned to the ORA, who then delivers it to the user, or directly to the user. Depending on the CA Operational Policy, the CA may actually return the certificate to both the ORA and the user, thus allowing the ORA to keep record of the certificates issued.

CAs shall operate in physically secure environments. The generation of CA private keys and the signing of certificates and CRLs shall occur within cryptographic modules as defined in FIPS 140-1 - *Security Requirements for Cryptographic Modules* [5].

4.2 Requirements for Low Assurance CAs

Low assurance CAs shall meet all the uniform requirements stated in Section 4.1. Low assurance CAs may only issue certificates that support low-risk applications, such as electronic mail. This type of certificate is not acceptable for applications that involve handling of personnel information or Government funds.

Low assurance CA may be implemented on systems conforming with FIPS 140-1 Level 2 security requirements and operated by a single CA agent. Equally the ORA(s) for a low assurance CA may be operated by a single ORA agent. Keys used for signing certificates shall never be exported in clear form and should reside in a hardware token under the control of the CA agent.

4.3 Requirements for Medium Assurance CAs

In addition to the uniform requirements stated in Section 4.1, medium assurance CAs shall meet the following requirements.

CA cryptographic modules must minimally conform to the Level 2 requirements of FIPS 140-1, with additional Level 3 requirements. The Level 2 and 3 requirements beyond the applicable Level 1 requirements are as follows:

- **Level 2 Physical Security:** All removable covers or doors shall be either locked with pick-resistant mechanical locks that employ physical or logical keys, or protected via tamper evident seals (e.g. evidence tape or holographic seals.) This requirement does not

prevent an intruder from gaining access to the module, however it does provide an alert that the module has been tampered with.

- **Level 2 Operating System Requirements:** If the module can only perform its intended CA functions and access to drives, other storage devices, and network (for loading software) is controlled, then the Operating System Requirements are not applicable. The same requirement may be waived if physical access to the system is restricted so that only vetted personnel with system maintenance or operation responsibilities may use the system and appropriate network controls are in place.

- **Level 3 Key Management Requirements:** Direct key entry for the input of unprotected key components shall be required.

Private keys shall either remain stored within a cryptographic module or be enciphered using DES (FIPS PUB 46-2 - *Data Encryption Standard*) [4] before being output. Security practices such as separation of privilege shall be employed. CA agents are instructed on the operation of the CA and provided with reference material on the proper use and safeguard of key material, audit logs, personal information, archival material, et cetera. Equally ORA agents are instructed on the operation of the ORA and provided with reference material on the proper use and safeguard of key material, audit logs, personal information, and archival material. Agents are also instructed on the rules and procedures for reporting lost or compromised keys.

4.4 Requirements for High Assurance CAs

In addition to the uniform requirements in Section 4.1, high assurance CAs shall meet the following requirements.

CA cryptographic modules must minimally conform to the Level 2 requirements of FIPS 140-1, with additional Level 3 requirements. The Level 2 and 3 requirements beyond the applicable Level 1 requirements are as follows:

- **Level 2 Physical Security:** All removable covers or doors shall be either locked with pick-resistant mechanical locks that employ physical or logical keys, or protected via tamper evident seals (e.g. evidence tape or holographic seals.) This requirement does not prevent an intruder from gaining access to the module, however it does provide an alert that the module has been tampered with.

- **Level 2 Operating System Requirements:** If the module can only perform its intended CA functions and access to drives, other storage devices, and network (for loading software) is controlled, then the Operating System Requirements in FIPS 140-1 are not applicable.

- **Level 3 Key Management Requirements:** Direct key entry for the input of unprotected key components shall be required.

- **Level 3 Roles and Services:** Identity-based authentication shall be enforced. Separate ports (or pins) shall be used to enter plaintext authentication data or keys.

Private keys shall either remain stored within a cryptographic module or be enciphered using DES (FIPS PUB 46-2 - *Data Encryption Standard*) [4] before being output. Security practices such as separation of privilege shall be employed. CAs shall only accept certificate requests signed by two different agents of the ORA. CA agents are instructed on the operation of the CA and provided with reference material on the proper use and safeguard of key material, audit logs, personal information, archival material, et cetera. Equally ORA agents are instructed on the operation of the ORA and provided with reference material on the proper use and safeguard of key material, audit logs, personal information, and archival material. Agents are also instructed on the rules and procedures for reporting lost or compromised keys.

5. Certificate Issuance Policies

Certificate issuance policies state the requirements or constraints under which certificates are issued. This includes: the personal identification requirements for users or other CAs being certified, procedures for the generation, safe keeping, revocation, and archiving of key material, an optional statement of the community for which the CA intends to issue certificates, etc.

The PAA shall evaluate other alternative policies and determine equivalence of new policies with existing issuance policies and assurance levels. Certificate issuance policies that will be used by two or more CAs shall be posted on the NIST Computer Security Objects Register (CSOR) [9].

5.1 CA Certificates

Identification and Authentication Requirements - For initial certification, CA representatives identify themselves to the certifying CA by presenting their id cards and an authorization letter from their organizations assigning them the responsibility for operation of the CA.

Certificate Renewal - CA certificate renewal requires an electronic request signed with the CA's current, unrevoked, private key. Initial CA certificates may be renewed once, i.e., the procedure for initial CA certification need only be performed every six years. Revoked certificates may not be renewed, replacement of revoked certificates shall follow the initial certification procedure.

Key Material - For initial certification the CA representative provides a self-signed skeleton certificate containing the public key on a 3.5" disk. For renewal the new key is transmitted in a

certificate request signed with the key being replaced. CA signature keys are 1024 bits long and valid for three years.

5.2 ORA Certificates.

Identification and Authentication Requirements - For initial certification, ORA representatives identify themselves to the certifying CA by presenting their id cards and an authorization letter from their organizations assigning them the responsibility for operation of the ORA.

Certificate Renewal - ORA certificate renewal requires an electronic request signed with the ORA's current, unrevoked, private key. Initial ORA certificates may be renewed twice, i.e., the procedure for initial ORA certification need only be performed every six years. Revoked certificates may not be renewed, replacement of revoked certificates shall follow the initial certification procedure.

Key Material - For initial certification the ORA representative provides a self-signed skeleton certificate (i.e., signed with the private key corresponding to the public key being certified) containing the public key on a 3.5" disk. For renewal, the new key is transmitted in a certificate request signed with the key being replaced. ORA signature keys are 1024 bits long and valid for two years.

5.3 Low Assurance User Certificate

Identification and Authentication Requirements - For initial certification, Government users requesting L-type certificates identify themselves to the ORA by presenting their Government identification card. Non-Government users requesting L-type certificates identify themselves by presenting any Federal, State, or Local Government picture identification such as valid drivers license, state-issued non-driver identification card, or passport. The ORA shall provide L-type certificate owners with instructions on the proper use and safeguard of their PKI clients and key material, including rules for reporting lost or compromised keys.

Certificate Renewal - L-type user certificate renewal requires an electronic request signed with the user's current, unrevoked, private key. Initial L-type certificates may be renewed once, i.e., the procedure for initial user certification need to be performed every two years. Revoked certificates may not be renewed, replacement of revoked certificates shall follow the initial certification procedure.

Key Material - For initial certification the user provides to the ORA a self-signed skeleton certificate (i.e., signed with the private key corresponding to the public key being certified) containing the public key on a 3.5" disk. For renewal, the new key is transmitted in a certificate request signed with the key being replaced. DSA keys associated with L-type certificates are at least 768 bits long (1024 bits maximum) and valid for one year.

5.4 Medium Assurance User Certificate

Identification and Authentication Requirements - For initial certification, Government users requesting M-type certificates identify themselves to the ORA by presenting their Government identification card. Non-Government users requesting M-type certificates identify themselves by presenting any Federal, State, or Local Government picture identification such as valid drivers license, state-issued non-driver identification card, or passport. In addition, these users shall present an authorization letter from their immediate supervisor or sponsor indicating that the user needs a medium assurance level certificate. The same letter may state locally defined qualifiers such as the user's role and other access control information. The ORA shall provide M-type certificate owners with instructions on the proper use and safeguard of their PKI clients and key material, including rules for reporting lost or compromised keys. Users are provided with instructions on the proper use and safeguard of their PKI clients and key material, including rules for reporting lost or compromised keys. New users are required to attend a half-hour briefing on the proper use of their client systems and their responsibilities in using and safeguarding their key material.

Certificate Renewal - M-type user certificate renewal requires an electronic request signed with the user's current, unrevoked, private key. Initial M-type certificates may be renewed once, i.e., the procedure for initial user certification need to be performed every four years. Revoked certificates may not be renewed, replacement of revoked certificates shall follow the initial certification procedure.

Key Material - For initial certification the user provides to the ORA a self-signed skeleton certificate (i.e., signed with the private key corresponding to the public key being certified) containing the public key on a 3.5" disk or a FIPS 140-1 Level 2 hardware cryptographic token. For renewal, the new key is transmitted in a certificate request signed with the key being replaced. DSA keys associated with M-type certificates are at least 896 bits long (1024 bits maximum) and valid for two years.

5.5 High Assurance User Certificate

Identification and Authentication Requirements - For initial certification, Government users requesting H-type certificates identify themselves to the ORA by presenting their Government identification card. Non-Government users requesting H-type certificates identify themselves by presenting any Federal, State, or Local Government picture identification such as valid drivers license, state-issued non-driver identification card, or passport. In addition, these users shall present an authorization letter from their immediate supervisor or sponsor indicating that the user needs a high assurance level certificate. The same letter may state locally defined qualifiers such as the user's role, authority to handle funds up to a predetermined amount, and other access control information. The ORA should confirm the authenticity of the letter with a telephone call. The ORA shall provide H-type certificate owners with instructions on the proper use and

safeguard of their PKI clients and key material, including rules for reporting lost or compromised keys. Users are provided with instructions on the proper use and safeguard of their PKI clients and key material, including rules for reporting lost or compromised keys. New users are required to attend a one-hour briefing on the proper use of their client systems and their responsibilities in using and safeguarding their key material.

All initial certificate requests for high assurance certificates shall be signed by two different agents of the ORA.

Certificate Renewal - H-type user certificate renewal requires an electronic request signed with the user's current, unrevoked, private key. Initial H-type certificates may be renewed once, i.e., the procedure for initial user certification need to be performed every four years. Revoked certificates may not be renewed, replacement of revoked certificates shall follow the initial certification procedure.

Key Material - For initial certification the user provides to the ORA a self-signed skeleton certificate (i.e., signed with the private key corresponding to the public key being certified) containing the public key on a FIPS 140-1 Level 3 (or higher) hardware cryptographic token. The cryptographic token shall be unable to export the signature private key. For renewal, the new key is transmitted in a certificate request signed with the key being replaced. DSA keys associated with H-type certificates are 1024 bits long and valid for two years.

6. Federal Assurance Levels

A Federal assurance level is an indication of the general level of trust that can be placed on a certificate, which will be broadly understood throughout the Federal PKI. The assessment of the trustworthiness of the information in a certificate is made by the PAA upon evaluating the policies and procedures followed by the certifying CA. Although Federal Assurance Levels will be conveyed in the certificate policy extension of Federal PKI certificates, they are not actual policies. A small set of Federal Assurance Level values (e.g., low, medium, high) will be registered by the CSOR under the certificate policies branch. A single Federal Assurance Level will be assigned to every certificate.

The PAA shall assess the trustworthiness of all Federal PKI CAs on a periodic basis. The frequency of these assessments will be determined by the PAA. The PAA's evaluation will be based on the guidelines outlined in this document. Upon request of the PAA, each CA shall:

- identify their target Federal Assurance Levels;
- identify the policies followed and where they are posted;
- identify the community or communities it serves;
- identify the equipment, Orange Book or equivalent rating, and FIPS 140-1 rating of the

cryptographic modules;
- identify physical and personnel security measures;
- identify the personnel involved in the operation of the CA, their roles, and what training have they received prior to operating the CA;
- identify the directory server, or servers, where the CA posts certificates and certificate revocation lists;
- provide documentation on the operational procedures of the CA (including initialization, backup, archive, audit, revocation, etc.);
- provide statistics on number of users and subordinate CAs, number and type of cross certificates, the volume of transactions, and average load due to revocation processing;
- allow the observation of actual day-to-day operations.

If a CA fails to implement certificate generation and maintenance procedures in accordance with the posted policies, or issues certificates identified with Federal Assurance Levels higher than those authorized by the PAA, its certificate and the cross certificate with its parent shall be revoked by the PAA.

7. Federal PKI Management

As stated in Section 2, although no structure is mandated for verification paths in the Federal PKI, the CAs that make up the Infrastructure are organized in a hierarchical fashion for administrative reasons. The CA at the top of the hierarchy is known as the Root CA and is associated with the Policy Approving Authority (PAA). The PAA is responsible for the integrity and trustworthiness of the Federal PKI. The PAA reviews CA policies and operational procedures to determine the Federal Assurance Levels that may be claimed on certificates created by a CA. After an initial assessment, the PAA performs periodic reviews of the operations of all the CAs in the Infrastructure to ensure that they meet the requirements of their own Operational and Certificate Issuing policies. CAs that fail to implement and maintain operational procedures that meet the requirements of its policies may find their certificates revoked by the PAA.

In order to supervise the operation of all CAs in the Federal PKI the PAA will call upon the management entities for several key CAs to assist in performing oversight functions for segments of the Infrastructure. The PAA will delegate oversight responsibilities to authorities selected based on geographical location, expertise, resources, et cetera. The distribution of the oversight responsibilities of the PAA should add flexibility and efficiency while ensuring even levels of quality for the different types of certificates granted by the Federal PKI regardless of the CA creating a certificate.

Since all trust in the Federal PKI is derived from the Root CA, the PAA also plays a role in setting naming and path length restrictions on other CAs. The PAA may also register new policies for use throughout the Infrastructure as necessary.

8. Records Keeping

Each CA shall log the following certification activities: request to create a certificate, certificates issued, request to revoke a certificate, generation of a CRL, and distribution of a CRL to the Directory. Once a week this information will be stored off-line for archival purposes. All archived information shall be maintained in a form that prevents unauthorized modification.

Every CA shall keep a separate audit log for the monitoring and tracking of security incidents.

9. CA Failure and Compromise Recovery

9.1 Backup Policy

All CAs and ORAs within the Federal PKI shall conduct daily system backups.

9.2 Notification Procedures

Upon occurrence of a system compromise or failure that may affect the integrity of the Infrastructure, the system affected shall obtain new certificates, issue the appropriate CRLs, and notify the affected parties of the need to re-authenticate to replace the compromised certificates.

9.3 Initialization Procedures

Upon system startup each CA shall obtain the certificates it needs from the parent CA and then issue certificates to all its users and subordinate CAs. As new certificates are generated, the directory server shall be notified in order to populate it with valid certificates. If the number of users is large, the process may take place in stages. When initialization occurs after a system compromise or failure, an effort shall be made to issue notifications to the subscribers if delays are expected to extend beyond 24 hours. Steps shall be taken to minimize the possibility of compromise and corruption at all levels of the Infrastructure and to expedite recovery procedures.

10. Certificate Revocation

A CA shall revoke a certificate upon validating a request from the certificate owner (a user, CA, or ORA), the ORA that requested the certificate, or the PAA. Common reasons for requesting revocation are: change of the owner's name, separation from the issuing organization, change of the privileges of the user, or failure by a CA to demonstrate compliance with its policies or to implement appropriate operational procedures.

User revocation requests may be directed to either the CA or the ORA. The CA shall accept electronic revocation requests signed with the compromised key, revocation requests presented in person, or through the telephone. All revocation requests shall be verified by the CA prior to taking effect. When the request is made in person, the user shall provide appropriate identification and the reason for the revocation. Revocation requests over the telephone shall only be accepted if a satisfactory personal identification can be made. To accomplish this, the CA or ORA could call back the user to the telephone number listed on the internal directory, establish a three-way telephone connection with the user's supervisor or agency sponsor, or request independent confirmation from the user's supervisor. If the private key was lost or compromised, the effective date and time for the revocation shall be provided. The CA shall issue an electronic notification of the request to the user's superior or agency sponsor. Electronic revocation requests also require verification by the CA.

After processing a request for revocation, the CA shall update and sign the CRL. CAs shall transmit CRLs to the directory twice daily, if any new revocations have occurred, or at least once every three days. CRLs shall always be signed with the issuing CA's valid private key. Expired certificates shall be deleted from the CRL.

Certificates are also revoked as part of recovery from compromise or database corruption. If the CA suspects database corruption, in addition to the key compromise, it shall revoke all subordinate certificates and electronically notify the subordinates. Old subordinate certificates need not be put on a CRL since the signatures on them will not verify. Subordinates can get the CA's new public key from the Directory.

Replacement of revoked certificates is accomplished by following the procedure used for initial registration. The CA shall reissue subordinate certificates using the new private key and post them to the Directory.

11. Cross Certification Guidelines

Cross certification is a mechanism in which two CAs grant each other certificates to signify a trust relationship. This differs from the strict hierarchy model where trust is passed down hierarchically along single certificate paths. The Federal PKI is organized as a hierarchy for administration purposes, but allows the establishment of cross certificates with some restrictions. The use of cross certificates allows the establishment of a network of trust relationships among CAs within and outside the Federal hierarchy.

The Federal PKI defines three types of cross certificates: hierarchical, general, and special. Hierarchical cross certificates parallel the hierarchical path from the Root CA. In the Federal PKI, every CA shall trust its parent CA. At certification time every CA shall cross certify its parent to ensure that signature verification engines that only follow cross certificates (i.e., do follow the

path from the root when verifying certificates) can verify signatures certified by the Federal PKI.

General cross certification is intended to simplify certificate paths for efficiency reasons (i.e., shorter verification paths). General cross certification shall not allow the circumvention of controls established hierarchically by the root and parent CAs through name, path length, and other restrictions. When performing a general cross certification, each CA verifies the path from the root to the CA being certified to determine the restrictions imposed by its hierarchy. The new cross certificate shall preserve those restrictions.

Special cross certification is intended to establish a relationship between two leaf CAs and their users that goes beyond the restrictions imposed by their hierarchies. For instance, they could relax the name restrictions imposed by the hierarchical path, or grant each other cross certificates with a Federal Assurance Level higher than that of the certificates granted by their respective parent CAs (given that they can demonstrate that they meet the appropriate criteria). Only leaf CAs are allowed to establish special cross certificates so that the circumvention of hierarchically imposed controls is limited to the users of the CAs involved.

12. Additional Services

12.1 Confidentiality Key Backup

The backup of confidentiality keys may be required to ensure that data can be recovered even if a key, or the token holding it, is lost or corrupted, to prevent loss of data when an employee leaves the organization without transferring control of the keys or of the plaintext data, or to protect against malicious action by disgruntled employees. Backup, or escrow, of confidentiality keys may also be required by law, regulation, or export controls.

Only keys used for the establishment of confidentiality-protected communication sessions or for the actual provision of data confidentiality services may be subject to back up or escrow by components of the Infrastructure. Private keys used for the generation of digital signatures shall not be subject to backup, escrow, or generation by any component of the Federal PKI. The generation of confidentiality keys shall occur on client systems or inside hardware tokens under the control of the user.

12.2 Secure Session Key Establishment

The Federal PKI shall provide for the existence of key material, bound to the owner, to be used in the establishment of session keys to provide confidentiality of interactive traffic and electronic messaging. A certificate, separate to the one containing the user signature public key shall be created to carry the confidentiality public key. The establishment of session keys is an operation between the communicating ends. The Federal PKI limits its involvement in the establishment of

such keys to providing and managing the necessary public key certificates.

13. References

1. ANSI X9.30-3, *Public Key Cryptography Using Irreversible Algorithms, Part 3: Certificate Management for DSA*, November 1993 (DRAFT).

2. Burr, W. E., *Federal PKI Concept of Operations*, Federal PKI Technical Working Group, November 1995, DRAFT.

3. CCITT X.500 Series (1992) | ISO/IEC 9594,1--9, *Information Technology -- Open Systems Interconnection -- The Directory*, 1992.

4. FIPS 46-2, *Data Encryption Standard* (DES), December 1993.

5. FIPS PUB 140-1, *Security Requirements for Cryptographic Modules*, January 1994.

6. FIPS PUB 180-1, *Secure Hash Standard* (SHS), National Institute of Standards and Technology, April 1995.

7. FIPS PUB 186 , *Digital Signature Standard* (DSS), National Institute of Standards and Technology, May 1994.

8. Internet RFC 1422, *Privacy Enhancement for Internet Electronic Mail: Part II Certificate-Based Key Management*, February 1993.

9. NISTIR 5308, N. Nazario, *General Procedures for Registering Computer Security Objects*, December 1993.

10. NIST Solicitation No. 52SBN5C8535, *NIST Public Key Infrastructure Pilot - RFC*, October 1994.

11. *Public Key Infrastructure Study*, The MITRE Corporation for the National Institute of Standards and Technology, April 1994.

Annex 1 - Quality Tests for DSA Key Material

At a minimum, the quality tests shall include:

- primality of p
- primality of q
- q divides evenly in p - 1
- $g > 1$
- $y < p$

Tests for the primality of *p* and *q* can be found in Appendix 2 of the DSS FIPS [9]. Additional tests will be available from NIST.

Annex 2 - Security Policy Object Definition

```
SecurityPolicyObject  ::= SEQUENCE {

    sPolicyID       SPolicyID,
    sPolicyItems    SPolicyItems }

SpolicyID           Object Identifier     --These policies will be
                                          --registered by the NIST CSOR
                                          --who will assign the OIDs.

SPolicyItems                ::= SEQUENCE{

    -- Spells out requirements for authenticating the
    -- certificate owner upon issue by the CMA.
    subjectAuthentication   [0] IMPLICIT OCTET STRING OPTIONAL,

    -- Indicates level of assurance of the issuing CMA system
    -- and its management procedures.
    cMAassurance                [1] IMPLICIT OCTET STRING
                                        OPTIONAL,

    -- Identifies the community served by the policy.
    communityServed         [2] IMPLICIT OCTET STRING OPTIONAL,

    --References applicable, laws, mandates, or regulations.
    legalRequirements           [3] IMPLICIT OCTET STRING OPTIONAL,

    -- Role or mission for which the certificate was created,
    -- e.g.,<individual, signature>, <individual, key exchange>,
    -- <financial officer, signature>.
    mission                     [4] IMPLICIT OCTET STRING OPTIONAL,

    -- Access control information.  An alternative to this would
    -- be a security label.
    accessControl               [5] IMPLICIT OCTET STRING OPTIONAL,

    -- The validity policy component may carry a time period
    -- or other specific condition.
    validity                    [6] IMPLICIT Validity OPTIONAL
```

```
    -- Associates a level of economic value to the policy and to
    -- the certificates generated under it.
    economicValue               [7] IMPLICIT EconomicValue
                                        OPTIONAL,

    -- States confidentiality-related protections and
    -- responsibilities of the system and the ceritificate
    -- holder.  An alternative to this would be a security
    -- label.
    confidentiality             [8] IMPLICIT OCTET STRING OPTIONAL,

    -- States integrity protections and responsibilities
    -- of the system and the ceritificate holder.  An
    -- alternative to this would be a security label.
    integrity                   [9] IMPLICIT OCTET STRING OPTIONAL,

    -- Statement of availability requirements and measures on
    -- systems under the policy.
    availability                [10] IMPLICIT OCTET STRING
                                        OPTIONAL,

    -- Security labels are defined in FIPS Pub 188 - Standard
    -- Security Label for Information Transfer (1994). Security
    -- labels can be used to convey access control and possibly
    -- confidentiality, integrity, community, validity, mission
    -- and value information.
    securityLabel               [11] IMPLICIT StandardSecurityLabel
                                        OPTIONAL
    }


Validity ::= CHOICE[
    tperiod     TPeriod,
    condition OCTET STRING }

Tperiod ::= SEQUENCE [
    startTime           UTCTime,
    endTime             UTCTime }

EconomicValue ::= SEQUENCE {
    lowerBound          REAL,
    upperBound          REAL }
```