United States Department of Defense
S-Interoperability Domain
X.509 Certificate Policy

Version 1

5 January 2012

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

1 INTRODUCTION

This Certificate Policy (CP) identifies the operations of the Multi-Domain Public Key Infrastructure (PKI) created by the S-Interop Root Certification Authority (CA).

The S-Interop PKI Domain is a hierarchical architecture, with the S-Interop Root CA at the top of the hierarchy. The S-Interop Root CA issues one-way cross-certificates to CAs (referred to as member CAs) that operate on National SECRET level networks to create the S-Interop Domain.

The issuance of a cross-certificate by the S-Interop Root CA to an external PKI does not imply approval for establishing connections between networks. It only facilitates trust of PKIs within networks which are approved for connection by other processes.

1.1 OVERVIEW

The S-Interop CP outlines the policy for the operation of the S-Interop Root CA and the procedures for the approval and issuance of cross-certificates to member CAs. This CP is modeled after the *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework* [RFC 3647].

Member CAs that are issued cross-certificates from the S-Interop Root CA operate under existing CPs and Certification Practice Statements (CPSs).

1.1.1 Certificate Policy

The S-Interop CP defines the policies asserted in cross-certificates issued by the S-Interop Root CA. All cross-certificates issued by the S-Interop Root CA shall contain a mapping from an S-Interop CP Object Identifier (OID) to one or more Policy OIDs supported by the member CA that may be used by a Relying Party to determine the security and technical controls of the policy under which an end entity certificate was issued.

The S-Interop CP is based on the *Committee on National Security Systems Instruction 1300 – Instruction for National Security Systems Public Key Infrastructure X.509 Certificate Policy* [NSS-PKI], and references [NSS-PKI] for many sections which have the same requirements. This CP provides specific requirements for the S-Interop Multi-Domain PKI where it differs from [NSS-PKI]. Where a section says “See [NSS-PKI],” [NSS-PKI] requirements apply to the S-Interop Root CA. Otherwise, the content of this CP directs the operations of the S-Interop Root CA.

1.1.2 Relationship between the Certificate Policy and the Certification Practice Statement

This S-Interop CP identifies the requirements for the operations of the S-Interop Root CA and the issuance of cross-certificates to member CAs. The S-Interop Root CA CPS states how the S-Interop Root CA meets those requirements. Member CAs are issued cross-certificates from the S-Interop Root CA and are expected to operate under existing CPs and CPSs.

1.1.3 Scope

This CP applies to the S-Interop Root CA and to the issuance of cross-certificates to member CAs operating in the S-Interop PKI Domain.

1.1.4 Interoperation with CAs Issuing Under Different Policies

The S-Interop Domain is defined by the set of CAs that have been issued one way cross-certificates by the S-Interop Root CA. The cross-certificate defines the policy mapping from an S-Interop CP OID to one or more CP OIDs asserted by the member CA. The issuance of cross-certificates will be performed under the direction of the DoD PKI Program Management Office (PMO).

1.2 DOCUMENT NAME AND IDENTIFICATION

The official title of the CP is the *United States Department of Defense S-Interoperability Domain X.509 Certificate Policy*.

The S-Interop Domain CP defines Certificate Policies. Each Certificate Policy has an OID, to be asserted in cross-certificate mappings to member CAs that comply with the stipulations related to that policy. The OIDs are registered under the id-infosec arc as:

> {joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101) dod(2) infosec(1) certificate-policy(11)}

id-US-dod-S-InteropHardware	ID::= {id-certificate-policy 32}
id-US-dod-S-InteropSoftware	ID::= {id-certificate-policy 33}
id-US-dod-S-InteropDevice	ID::= {id-certificate-policy 34}

The stipulations presented in this CP apply to all OIDs unless otherwise noted.

This CP is the authoritative source for the definition and assignment of Policy OIDs for the S-Interop Domain.

The S-Interop Root CA may include these OIDs in end entity certificates necessary for operation (to include Online Certificate Status Protocol (OCSP) delegated trust model certificates). The S-Interop Root CA shall conform to the requirements specified in [NSS-PKI] for issuing end entity certificates. The following provides the comparability between S-Interop Domain and [NSS-PKI] OIDs:

id-CNSS-hardware	*id-US-dod-S-InteropHardware*
id-CNSS-software	*id-US-dod-S-InteropSoftware*
id-CNSS-device	*id-US-dod-S-InteropDevice*

For cross certificates:

The *id-US-dod-S-InteropDevice* OID shall only be used in cross certificates which map to a member policy OID that is only for devices.

The *id-US-dod-S-InteropHardware* and *id-US-dod-S-InteropSoftware* OIDs may be used for certificates issued to people, roles or devices.

1.3 PKI PARTICIPANTS

The following sections introduce the entities that participate in the S-Interop Domain. Responsibilities, qualifications, and additional controls for individuals designated as holding a trusted role are described in detail in Section 5.2.

1.3.1 Policy Management

The Policy Management Authority (PMA) for the S-Interop Domain is the Director, DoD PKI PMO. The PMA has the following responsibilities:

- Approve this S-Interop CP;
- Approve the S-Interop Root CA CPS; and,
- Approve the issuance of cross-certificates from the S-Interop Root CA to member CAs.

1.3.2 Certification Authorities

The S-Interop Root CA is the trust anchor for the S-Interop Domain. The S-Interop Root CA is responsible for issuing and managing cross-certificates including the following:

- The cross-certificate manufacturing and issuance process;
- Publication of its own signing certificate and cross-certificates;
- Revocation of cross-certificates;
- Publication of CRLs; and,
- Ensuring that all aspects of the Root CA services, operations, and infrastructure related to certificates issued under this CP are performed in accordance with the requirements, representations, and warranties of this CP.

A member CA is a CA that has been issued a cross-certificate from the S-Interop Root CA. Member CAs issue certificates to subordinate CAs and end entities (e.g., people, devices).

1.3.3 Registration Authority

The S-Interop Root CA does not use the services of Registration Authorities. Operations of the S-Interop Root CA, including the issuance of cross-certificates, are performed by CA Operations staff.

1.3.4 Subscriber

A Subscriber is the entity whose name appears as the subject in a certificate. While CAs are technically named in certificates, the term only refers to end entities and not certificate issuers. The S-Interop Root CA does not directly issue subscriber certificates. A subscriber in the S-Interop Domain is any end entity that has been issued a certificate by a member CA that has been issued a cross-certificate by the S-Interop Root CA or is subordinate to such a CA.

1.3.5 Relying Party

A Relying Party uses a Subscriber's certificate to verify or establish one or more of the following:

- The identity and status of an individual, role, system or device;
- The integrity of a digitally signed message;
- The identity of the creator of a message; and,
- Confidential communications with the Subscriber.

A Relying Party is the entity that relies on the validity of the binding of the Subscriber's name to a public key. A 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 OIDs) to determine the suitability of the certificate for a particular use.

Relying Parties may base the reliance they choose to place on a certificate on factors such as the amount and type of inherent risk of an activity, the consequence of failure, and the use of risk mitigation controls.

A Relying Party to the S-Interop Domain is defined as a party that has established direct trust in the S-Interop Root CA and thus trusts all certificates issued by member CAs and their subordinate CAs. Parties who directly trust a CA that is also cross certified but do not directly trust the S-Interop Root CA are not considered Relying Parties of the S-Interop Domain.

1.3.6 Other Participants

The S-Interop Root CA may require the services of other security, community, and application authorities, such as compliance auditors. These authorities, their services, and the mechanisms used to support their services shall be identified.

1.4 CERTIFICATE USAGE

PKIs can support the following security services: confidentiality, integrity, authentication, and technical non-repudiation. PKIs support the authentication, integrity, and technical non-repudiation security services through digital signatures, and the confidentiality security service through encryption. These basic security services support the long-term integrity of application data, but by themselves may not provide a sufficient integrity solution for all application circumstances.

1.4.1 Appropriate Certificate Uses

Certificates issued under this policy are used to determine the mapping from the member CA CP to the S-Interop CP and are intended to be used to facilitate protection of information classified at SECRET or below within SECRET networks or information systems.

1.4.2 Prohibited Certificate Uses

Certificates issued under this CP shall not be used other than to support transactions related to United States (U.S.) Government business.

1.5 POLICY ADMINISTRATION

1.5.1 Organization Administering the Document

The PMA is responsible for all aspects of this CP.

1.5.2 Contact Person

Questions regarding this CP should be directed to:

DOD PKI PROGRAM MANAGEMENT OFFICE
9800 SAVAGE RD STE 6718
FT GEORGE G MEADE MD 20755-6718

1.5.3 Person Determining CPS Suitability for the Policy

The PMA shall affirm the suitability of the S-Interop Root CA CPS to this policy.

1.5.4 CPS Approval Procedures

The S-Interop Root CA shall be operated in conformance with the S-Interop Root CA CPS. This CPS shall be conformant with the NSS Root CA CPS except for requirements related to the issuance of cross-certificates (Sections 1.1.4, 1.2, 1.3.1.1, 1.3.1.2 and 3.2.6), where it shall conform to the stipulations of this CP.

All member CAs shall operate in conformance with CPSs that have been approved as meeting the requirements of their associated CPs.

1.5.5 Waivers

See [NSS-PKI].

1.6 DEFINITIONS AND ACRONYMS

See Appendices B and C.

2 PUBLICATIONS AND REPOSITORY RESPONSIBILITIES

2.1 REPOSITORIES

The S-Interop Root CA and each cross-certified member CA shall maintain a repository that supports HTTP or LDAP to provide CA certificates and CRLs. Member CA repositories shall be operated such that expected relying parties have access to necessary data at least 95% of the time.

2.2 PUBLICATION OF CERTIFICATION INFORMATION

The S-Interop Root CA and each cross-certified member CA shall provide an on-line repository that is available to Subscribers and Relying Parties and that contains:

- The CA's signing certificate;
- Any Subordinate CA signing certificates;
- The most recent CRL for the CA and any Subordinate CAs; and,
- The CP that governs the operations of the CA.

In addition, the S-Interop Root CA shall provide the following:

- This S-Interop CP;
- All cross-certificates issued by the S-Interop Root CA; and,
- A list of entities that have been issued cross-certificates, along with information about obtaining information from the on-line repositories for those member CAs.

2.3 TIME OR FREQUENCY OF PUBLICATION

S-Interpop Root CA requirements for posting of revocation data are contained in Sections 4.9.7 and 4.9.8. The DoD NSS-PKI repository shall obtain information from the S-Interop Root CA repository at least every six hours.

2.4 ACCESS CONTROLS ON REPOSITORIES

See [NSS-PKI].

3 IDENTIFICATION AND AUTHENTICATION

3.1 NAMING

3.1.1 Types of Names

The S-Interop Root CA's signing certificate and all cross-certificates shall contain the issuer DN of the S-Interop Root CA and a subject DN indicating the name of the cross-certified CA.

3.1.2 Need for Names to be Meaningful

See [NSS-PKI].

3.1.3 Anonymity or Pseudonymity of Subscribers

See [NSS-PKI].

3.1.4 Rules for Interpreting Various Name Forms

See [NSS-PKI].

3.1.5 Uniqueness of Names

The PMA shall ensure that all cross-certificates issued by the S-Interop Root CA enforce name uniqueness.

3.1.6 Recognition, Authentication and Role of Trademarks

The S-Interop Root CA shall not knowingly issue a certificate that contains a trademark in the name. The S-Interop Root CA is not obligated to research trademarks or resolve trademark disputes.

3.2 INITIAL IDENTITY VALIDATION

3.2.1 Method to Prove Possession of Private Key

Requests for cross-certificates shall be made in a PKCS #10 format which is signed by the private key. The S-Interop Root CA will verify the signature on the self-signed certificate request it receives using the public key contained in the request.

3.2.2 Authentication of Organization Identity

Requests for cross-certificates shall include the CA name, address, and documentation for the existence of the CA. Before issuing a cross-certificate, an authority for the S-Interop Root CA shall verify the information, in addition to verifying the identity of the requesting representative and the authorization of that representative to act in the name of the CA as specified in Sections 4.1 and 4.2.

3.2.3 Authentication of Individual Identity

Requests for cross certificates shall be approved by the PMA prior to issuance. The PMA shall provide to the S-Interop Root CA personnel cross-certificate attributes including approved Policy OIDs, DN, and any name space constraints. The PMA shall also provide name and contact information for two representatives designated to request the cross-certificate from the external PKI.

3.2.4 Non-Verified Subscriber Information

Information that is not verified shall not be included in certificates.

3.2.5 Validation of Authority

Prior to issuing a cross-certificate, the S-Interop Root CA shall verify that the PMA has authorized the issuance of the cross-certificate to the member CA and the authority of the requesting representative to act in the name of the member CA as specified in Sections 4.1 and 4.2.

3.2.6 Criteria for Interoperation

The decision to include a member CA in the S-Interop Domain shall reside with the PMA. Unless there is a separately agreed standard (e.g., *Combined Communications Electronics Board (CCEB) Pub 1010 – PKI Cross-Certification Between CCEB Nations*), [NSS-PKI] shall be used to evaluate the comparability of a potential member CP along with specific requirements for member CAs specified in this CP. Prior to the issuance of a cross-certificate, the PMA shall execute a Memorandum of Agreement (MOA) with the PMA for the member CA that indicates the terms of the cross-certification agreement.

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

Not Applicable.

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

Revocation requests shall be authenticated. See Section 4.9.3.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

4.1.1 Who Can Submit a Certificate Application

The S-Interop Root CA shall only accept certificate requests submitted under two person control by the authorized representatives of the external PKI. S-Interop Root CA personnel shall verify that the public key in the cross certificate request matches the published Public key of the member Nation PKI CA that is the subject of the request.

4.1.2 Enrollment Process and Responsibilities

The S-Interop Root CA shall not issue a cross-certificate until authorized by the PMA. The PMA shall provide the S-Interop Root CA with the identities of the authorized representatives and all specific information necessary for the execution of the cross certificate. The S-Interop Root CA shall ensure two person control of the issuance process from acceptance of the cross-certificate request through issuance.

4.2 CERTIFICATE APPLICATION PROCESS

4.2.1 Performing Identification and Authentication Functions

S-Interop Root CA personnel shall authenticate all communications related to issuance of cross certificates. All communications between the S-Interop Root CA, the PMA and the external PKI requesting a cross-certificate shall be authenticated and protected from modification using mechanisms commensurate with the requirements of the data to be protected by the certificates being issued. Any electronic transmission of shared secrets shall be protected (e.g., encrypted) using means commensurate with the requirements of the data to be protected by the certificates being issued. To the extent possible, communications shall be performed on classified networks. The PMA and trusted roles of the S-Interop Root CA shall use NSS-PKI certificates for electronic communications for communications on SECRET networks and certificates issued by the DoD PKI for communications on UNCLASSIFIED networks.

4.2.2 Approval or Rejection of Certificate Applications

Cross-certificates shall only be issued upon approval from the PMA. A certificate application is not considered accepted until the S-Interop Root CA has accepted the application and issued a certificate.

4.2.3 Time to Process Certificate Applications

No stipulation.

4.3 CERTIFICATE ISSUANCE

4.3.1 CA Actions during Certificate Issuance

The S-Interop Root CA shall ensure that the certificate request has been authenticated and validated, obtain a proof of possession of the private key by validating the signature of the PKCS#10, and then generate a certificate and provide the certificate to the representative of the member CA.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

The S-Interop Root CA shall notify the member CA representative of certificate issuance.

4.4 CERTIFICATE ACCEPTANCE

4.4.1 Conduct Constituting Certificate Acceptance

Providing the certificate to the representative of the member CA shall constitute cross-certificate acceptance.

4.4.2 Publication of the Certificate by the CA

See Section 2.2.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

The S-Interop Root CA shall notify the PMA that the certificate was issued and post notice of the issuance of the cross-certificate to the member CA to the S-Interop Root CA Repository.

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 Subscriber Private Key and Certificate Usage

See [NSS-PKI].

4.5.2 Relying Party Public Key and Certificate Usage

A Relying Party should only use a public key for the purposes indicated in the certificate *Key Usage* extension. Relying Parties should not use expired or revoked encryption certificates. If the *Extended Key Usage* extension is present and implies any limitation on the use of the certificate, those constraints should also be followed.

4.6 CERTIFICATE RENEWAL

Not Applicable.

4.7 CERTIFICATE RE-KEY

Not Applicable.

4.8 CERTIFICATE MODIFICATION

Not Applicable.

4.9 CERTIFICATE REVOCATION AND SUSPENSION

The S-Interop Root CA shall authenticate all revocation requests.

4.9.1 Circumstances for Revocation

The S-Interop Root CA shall revoke cross-certificates if any of the following circumstances occur:

- The member CA no longer desires to be a part of the S-Interop Domain;
- The PMA no longer desires the member CA to be a member of the S-Interop Domain;
- The member CA is not meeting the stipulations of its own CPS or CP;
- The member CA is not meeting the stipulations of the MOA or other agreement signed as part of the cross-certificate issuance process; or,
- The member CA’s own signing key is compromised or there is reason to believe that the signing key has been compromised.

4.9.2 Who Can Request a Revocation

The PMA may request revocation of any cross-certificate issued by the S-Interop Root CA. The member CA may request revocation of its own cross-certificate. The persons authorized to request revocation of the member CA cross-certificate shall be identified in the cross-certificate MOU.

If the S-Interop Root CA determines that a cross-certified CA is not meeting the requirements of this CP, or a situation has occurred that may affect the integrity of the S-Interop Domain, the S-Interop Root CA is authorized to revoke the cross-certificate. Where possible, the S-Interop Root CA shall first attempt to resolve the issue without revoking the certificate.

4.9.3 Procedure for Revocation Request

Any format that is used to request a revocation shall identify the certificate to be revoked, explain the reason for revocation, and allow the request to be authenticated (e.g., digitally or manually signed). All revocation requests shall be verified to ensure that they have appropriate justification and are authentic to prevent malicious revocation of certificates by unauthorized parties.

The S-Interop Root 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. Revoked certificates shall be included on at least one CRL, and shall be included on all new publications of the CRL until the certificates expire. Revocation takes effect upon initial publication of the CRL containing the revocation information.

The S-Interop Root CA shall update the repository of the status of the member CA after revocation of a cross-certificate.

4.9.4 Revocation Request Grace Period

There is no grace period for revocation.

4.9.5 Time within Which CA Must Process the Revocation Request

The S-Interop Root CA shall complete processing of a revocation request within 1 hour of receipt of a properly authenticated and verified request.

4.9.6 Revocation Checking Requirements for Relying Parties

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 the Relying Party. Revocation data should be obtained from an authoritative source, such as a CRL.

If it is temporarily infeasible to obtain revocation information from an authoritative source, then the Relying Party should either reject use of the certificate or make an informed decision to accept the risk, responsibility, and consequences for using a certificate whose authenticity cannot be guaranteed to the standards of this policy.

4.9.7 CRL Issuance Frequency

The S-Interop Root CA shall issue a CRL at least once every 31 days or immediately after completion of processing a revocation of a cross-certificate for any reason.

The S-Interop Root CA shall ensure that superseded CRLs are removed from the repository upon posting of the latest CRL.

4.9.8 Maximum Latency for CRLs

In order to ensure that Relying Parties may obtain a current, valid CRL, the time indicated in the *nextUpdate* field of the CRL shall be past the time indicated in the *thisUpdate* field by a minimum of one day; and not past the time indicated in the *thisUpdate* field by more than seven days.

4.9.9 On-line Revocation/Status Checking Availability

See Section 4.10.

4.9.10 On-line Revocation Checking Requirements

See Section 4.10.

4.9.11 Other Forms of Revocation Advertisements Available

No stipulation.

4.9.12 Special Requirements Related to Key Compromise

See Sections 4.9.7 and 5.7.1 for incident and compromise handling and Section 5.7.3 for entity private key compromise procedures. See Section 4.9.3 for revocation procedures.

4.9.13 Certificate Suspension and Restoration

The S-Interop Root CA shall not support certificate suspension and restoration.

4.10 CERTIFICATE STATUS SERVICES

The S-Interop Domain shall not operate separate Certificate Status Services. The S-Interop Root CA may issue delegated trust model certificates to OCSP Responders operated under [NSS-PKI].

4.11 END OF SUBSCRIPTION

Subscription is synonymous with the cross-certificate validity period. The subscription ends when the cross-certificate expires or is revoked.

4.12 KEY ESCROW AND RECOVERY

The S-Interop Root CA shall not support key escrow and recovery.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 PHYSICAL CONTROLS

See [NSS-PKI].

5.2 PROCEDURAL CONTROLS

See [NSS-PKI].

5.3 PERSONNEL CONTROLS

See [NSS-PKI].

5.4 AUDIT LOGGING REQUIREMENTS

See [NSS-PKI].

5.5 RECORDS ARCHIVAL

See [NSS-PKI].

5.6 KEY CHANGEOVER

See Section 6.1.4 for information on delivery of the S-Interop Root CA certificate.

5.7 COMPROMISE AND DISASTER RECOVERY

5.7.1 Incident and Compromise Handling Procedures

If some form of potential compromise of the signing key for the S-Interop Root CA becomes known, the PMA shall perform an investigation to determine the nature and the degree of damage. If warranted, the S-Interop Root CA shall be re-keyed and all cross-certificates shall be re-issued in accordance with Section 5.7.3.

If some form of potential compromise of the signing key for a member CA becomes known, a representative from the member CA shall notify the PMA of the potential compromise. If warranted, the S-Interop Root CA shall revoke the cross-certificate issued to the member CA in accordance with Section 4.9.

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

For the S-Interop Root CA, see [NSS-PKI]. For member CAs, shall respond as follows when computing resources, software, and/or data are corrupted:

- Notify the PMA and cross-certified partners as soon as possible;
- Ensure that the system's integrity has been restored prior to returning to operation and determine the extent of risk due to operations since the last point of backup;
- If the member CA signing keys are not destroyed, the integrity of the system has been restored, and the risk is deemed negligible, reestablish CA operations, giving priority to the ability to generate certificate status information within the CRL issuance schedule specified in Section 4.9.7;
- If the member CA signing keys are destroyed, the integrity of the system cannot be restored, or the risk is deemed substantial, reestablish CA operations as quickly as possible, giving priority to the generation of a new CA signing key pair; and,
- If new member CA signing keys are issued, the member CA's PMA shall request revocation of current cross certificate and may initiate the process for obtaining a new cross-certificate.

5.7.3 Entity Private Key Compromise Procedures

In the case of the S-Interop Root CA compromise, the PMA shall, within 6 hours of determination of loss or compromise, notify all member CAs that have been issued cross-certificates by the S-Interop Root CA so that they can notify all Relying Parties to remove the trusted self-signed certificate from their trust stores. Initiation of notification shall be made in an authenticated and trusted manner. The PMA shall then re-establish the S-Interop Domain by generating a new S-Interop Root CA certificate, issuing new cross-certificates, and securely distributing the new Root CA certificate as specified in Section 6.1.4.

In the case of a member CA compromise, the member CA's PMA shall immediately request the revocation of the cross-certificate and, once the member CA has been reestablished, may initiate the process for obtaining a new cross certificate.

5.7.4 Business Continuity Capabilities after a Disaster

See [NSS-PKI].

5.8 CA, RA, OR TA TERMINATION

See [NSS-PKI] for CA termination. The S-Interop Root CA does not use the services of RAs or TAs.

6 TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 Key Pair Generation

See [NSS-PKI].

6.1.2 Private Key Delivery to Subscriber

Not Applicable.

6.1.3 Public Key Delivery to Certificate Issuer

Public keys shall be delivered to the S-Interop Root CA in a signed PKCS#10 request.

6.1.4 CA Public Key Delivery to Relying Parties

See [NSS-PKI].

6.1.5 Key Sizes

See [NSS-PKI].

6.1.6 Public Key Parameters Generation and Quality Checking

See [NSS-PKI].

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

See [NSS-PKI].

6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

See [NSS-PKI].

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1 Public Key Archival

See [NSS-PKI].

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The S-Interop Root CA shall not issue a cross-certificate that extends beyond the expiration date of its own certificate. Cross-certificates shall have a maximum validity period of three years.

6.4 ACTIVATION DATA

See [NSS-PKI].

6.5 COMPUTER SECURITY CONTROLS

See [NSS-PKI].

6.6 LIFE CYCLE TECHNICAL CONTROLS

See [NSS-PKI].

6.7 NETWORK SECURITY CONTROLS

See [NSS-PKI].

6.8 TIME STAMPING

See [NSS-PKI].

7 CERTIFICATE, CSP, AND OCSP PROFILE

7.1 CERTIFICATE PROFILE

See *Committee on National Security Systems (CNSS) Public Key Infrastructure (PKI) Certificate Profiles* [NSS-Prof].

S-Interop Domain cross-certificates shall include mechanisms that limit transitive trust.

Any variance of this profile shall be approved by the PMA, and documented in a CPS.

7.2 CRL PROFILE

See [NSS-Prof]. Any variance of this profile shall be approved by the PMA, and documented in a CPS.

7.3 OCSP PROFILE

No stipulation.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 FREQUENCY AND CIRCUMSTANCES OF ASSESSMENT

See [NSS-PKI].

8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR

See [NSS-PKI].

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

See [NSS-PKI].

8.4 TOPICS COVERED BY ASSESSMENT

For the S-Interop Root CA, see [NSS-PKI]. The purpose of the compliance audit shall be to verify that the audited party has in place a system to assure the quality of the services that it provides, and that it complies with all the requirements of the current versions of its CP and CPS. All aspects of the audited party's operations related to its CP and CPS shall be subject to compliance audit inspections.

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

See [NSS-PKI].

8.6 COMMUNICATION OF RESULTS

For the S-Interop Root CA, see [NSS-PKI]. The member CA shall provide an audit summary report to the PMA indicating any discrepancies identified during the audit that were not able to be resolved, and indicating any critical failures that would contribute to the ongoing compromise of information.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 FEES

Member CAs shall make current revocation information, including CRLs, available to Relying Parties at no charge.

9.2 FINANCIAL RESPONSIBILITY

Relying Parties should determine, within their purview, what financial limits if any they wish to impose for the reliance on certificates used to consummate a transaction; and shall implement applications as appropriate to support those limitations. The PMA assumes no financial responsibility or liability for those decisions.

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

See [NSS-PKI].

9.4 PRIVACY OF PERSONAL INFORMATION

See [NSS-PKI].

9.5 INTELLECTUAL PROPERTY RIGHTS

See [NSS-PKI].

9.6 REPRESENTATIONS AND WARRANTIES

See [NSS-PKI].

9.7 DISCLAIMERS OF WARRANTIES

See [NSS-PKI].

9.8 LIMITATIONS OF LIABILITY

The DoD and U.S. Government shall not be liable to any party for the operation of the S-Interop Root CA.

9.9 INDEMNITIES

No stipulation.

9.10 TERM AND TERMINATION

9.10.1 Term

This S-Interop CP becomes effective when approved by the PMA. It shall remain in effect until either a new S-Interop CP is approved by the PMA or the S-Interop Root CA is terminated.

9.10.2 Termination

This CP shall survive any termination of the S-Interop Root CA. The requirements of this CP remain in effect through the end of the archive period for the last certificate issued by the S-Interop Root CA.

9.10.3 Effect of Termination and Survival

The responsibilities for protecting business confidential and personal information, and for protecting intellectual property rights, shall survive termination of this CP.

Intellectual property rights shall survive this CP in accordance with the Intellectual Property laws of the United States.

The archive requirements of this CP remain in effect through the end of the archive period for the last certificate issued. Other requirements concerning the operation of the S-Interop Root CA shall remain in effect through the expiration date or revocation of the last cross-certificate issued and/or cessation of operations and closure of the S-Interop Domain.

9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

The PMA shall establish appropriate procedures for communications with member CAs that have been issued cross-certificates by the S-Interop Root CA.

9.12 AMENDMENTS

9.12.1 Procedure for Amendment

The PMA shall maintain this S-Interop CP. Any suggested changes shall be communicated to the contact in Section 1.5.2. All such communication shall include a description of the change, a change justification, and contact information for the person requesting the change.

9.12.2 Notification Mechanism and Period

Changes shall be incorporated into an updated version of this S-Interop CP, which shall be published to the repository in accordance with Section 2.

9.12.3 Circumstances under which OID Must be Changed

CP OIDs shall only change if the change in the S-Interop CP results in a material change to the trust by Relying Parties.

9.13 DISPUTE RESOLUTION PROVISIONS

The PMA shall decide any disputes over the issuance or revocation of cross-certificates by the S-Interop Root CA.

9.14 GOVERNING LAW

The operations of the S-Interop Root CA shall be governed by U.S. Federal law (statute, case law), or regulations, directives or policies.

9.15 COMPLIANCE WITH APPLICABLE LAW

No stipulation beyond requirements identified in CPs and CPSs for member CAs.

9.16 MISCELLANEOUS PROVISIONS

No stipulation beyond requirements identified in CPs and CPSs for member CAs.

9.17 OTHER PROVISIONS

No stipulation.

APPENDIX A REFERENCES

Reference	Title
ABA DSG	American Bar Association, *Digital Signature Guidelines*, 1 August 1996
CNSS 4009	Committee on National Security Systems Instruction 4009, *National Information Assurance (IA) Glossary*, 26 April 2010
NSS-PKI	Committee on National Security Systems Instruction 1300, *Instruction for National Security Systems Public Key Infrastructure X.509 Certificate Policy*, June 2011
NSS-Prof	*Committee on National Security Systems (CNSS) Public Key Infrastructure (PKI) Certificate Profiles*
RFC 3647	Internet Engineering Task Force, *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*, November 2003
SP 800-57	NIST Special Publication 800-57, *Recommendation for Key Management – Part 1: General* National Institute for Standards and Technology, May 2011

APPENDIX B ACRONYMS AND ABBREVIATIONS

ANMA	Agency NSS PKI Management Authority
AES	Advanced Encryption Standard
AIA	Authority Information Access
CA	Certification Authority
CAS	Certification Authority System
CMCS	COMSEC Material Control System
CMMI	Capability Maturity Model Integration
CNSS	Committee for National Security Systems
CNSSP	CNSS Policy
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSOR	Computer Security Objects Register
CSS	Certificate Status Server
dc	Domain Component
DIRNSA	Director, National Security Agency
DN	Distinguished Name
FIPS	Federal Information Processing Standard
HTTP	Hyper Text Transfer Protocol
IA	International Alphabet
ID	Identification
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IP	Internet Protocol
ITU	International Telecommunications Union
KES	Key Escrow System
LDAP	Lightweight Directory Access Protocol
MOA	Memorandum of Agreement
NIST	National Institute for Standards and Technology
NSA	National Security Agency
NSD	National Security Directive
NSS PKI	National Security Systems PKI
OCSP	Online Certificate Status Protocol
ODNI	Office of the Director of National Intelligence
OID	Object Identifier
PIN	Personal Identification Number
PIV	Personal Identity Verification

PKI	Public Key Infrastructure
PMA	Policy Management Authority
POC	Point of Contact
RA	Registration Authority
RPS	Registration Practice Statement
SSBI	Single Scope Background Investigation
TA	Trusted Agent
TLS	Transport Layer Security
U.S.	United States
UTF	Unicode Transformation Format

APPENDIX C GLOSSARY OF TERMS

Term	Definition
Activation Data	A pass-phrase, Personal Identification Number (PIN), biometric data, or other mechanisms of equivalent authentication robustness used to protect access to any use of a private key, except for private keys associated with System or Device certificates.
Agency NSS PKI Management Authority (ANMA)	The entity within an agency that operates a CA under this policy that is responsible for all aspects of management of the NSS PKI program for that agency, and for participating in the NSS PKI Member Governing Body.
Agency NSS PKI Point of Contact (POC)	The entity within an agency that does not operate a CA under this policy but that obtains certificates from a Common Services Provider CA operated under this policy. The POC is responsible for all aspects of management of the NSS PKI program for that agency and is responsible for participating in the NSS PKI Member Governing Body.
Agency Repository	A repository maintained by each agency that operates a CA. The repository shall support HTTP or LDAP to provide CA certificates and CRLs and collects information from the central repository for use by systems on that agency's network.
Authentication	Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information. [CNSS 4009]; A process used to confirm the identity of a person or to prove the integrity of specific information
AutoEnroll Certificates	Certificates issued to systems and devices that can only authenticate to the CA using their identifier and password, and cannot authenticate using their NSS PKI certificates.
Bits of Security	See Security Strength.
Central Repository	A repository that provides CA certificates and CRLs that supports overall NSS PKI operations with both HTTP and LDAP interfaces. The central repository function may consist of one or more repositories to support overall NSS PKI operations at the discretion of the NSS PKI Member Governing Body or the PMA. The central repository shall collect necessary information from the agency repositories.
Certificate	A digital representation of information which at least • Identifies the certification authority issuing it • Names or identifies its Subscriber • Contains the Subscriber's public key • Identifies its operational period, and (5) is digitally signed by the certification authority issuing it. [ABA DSG]
Certification Authority (CA)	An entity authorized to create, sign, and issue public key certificates.
Certification Authority System (CAS)	The collection of hardware, software, and operating personnel that create, sign, and issue public key certificates to Subscribers.
Certificate Policy (CP)	A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular CP might indicate applicability of a type of certificate to the authentication of parties engaging in business-to-business transactions for the trading of goods or services within a given price range. [RFC 3647]

Term	Definition
Certificate Policy OID	The certificate policy object identifier (OID) is a numeric string that is used to uniquely identify the set of certificate policy requirements stipulated in a CP.
Certificate Revocation List (CRL)	These are digitally signed “blacklists” of revoked certificates. CAs periodically issue CRLs, and users can retrieve them on demand via repositories.
Certificate Status Server (CSS)	An authority that provides status information about certificates on behalf of the CA through online transactions (e.g., an Online Certificate Status Protocol (OCSP) responder).
Certification Practice Statement (CPS)	A document representing a statement of practices a CA employs in issuing certificates.
CNSS	Committee on National Security Systems, a U.S. government organization providing guidance for the security of national security systems.
Code Signing Certificate	A certificate issued for the purpose of digitally signing executables and scripts to confirm the software author and guarantee that the code has not been altered or corrupted since it was signed by use of a cryptographic hash.
Common Services Provider	A provider of services, typically CA services, to agencies that do not operate their own CA.
Confidentiality	Assurance that information is not disclosed to unauthorized entities or processes. [CNSS 4009]
Content Signing Certificate	A certificate issued for the purpose of digitally signing information (content) to confirm the author and guarantee that the content has not been altered or corrupted since it was signed by use of a cryptographic hash.
Cross Certificate	A certificate issued from a CA that signs the public key of another CA not within its trust hierarchy that establishes a trust relationship between the two CAs. {Note: This is a more narrow definition than described in X.509.}
Edge Device Certificates	Certificates issued to support dual tunneling as part of a solution for protecting SECRET classified data traversing an unprotected network.
Encryption Certificate	A certificate containing a public key that can encrypt or decrypt electronic messages, files, documents, or data transmissions, or establish or exchange a session key for these same purposes. Key management sometimes refers to the process of storing protecting and escrowing the private component of the key pair associated with the encryption certificate.
Identity Certificate	A certificate that provides authentication of the identity claimed. Within the NSS PKI, identity certificates may be used only for authentication or may be used for both authentication and digital signatures.
Integrity	Protection against unauthorized modification or destruction of information. [CNSS 4009]
Intermediate Certification Authority (CA)	A CA that is signed by a superior CA (e.g., a Root CA or another Intermediate CA) and signs CAs (e.g., another Intermediate or Subordinate CA). The Intermediate CA exists in the middle of a trust chain between the Trust Anchor, or Root CA, and the subscriber certificate issuing Subordinate CAs.
Key Compromise	Disclosure of the private key to unauthorized persons, or a violation of the security policy of the PKI in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of the private key may have occurred.
Key Escrow	The retention of the private component of the key pair associated with a Subscriber’s encryption certificate to support key recovery.

Term	Definition
Key Escrow System (KES)	The system responsible for storing and providing a mechanism for obtaining copies of private keys associated with encryption certificates, which are necessary for the recovery of encrypted data.
Key Recovery	The process for obtaining a copy of an escrowed private key from the KES.
Legacy NSS PKI	An operational PKI on an agency's classified network prior to the establishment of the NSS PKI.
Modification	The process of creating a new certificate with a new serial number that differs in one or more fields from the old certificate. The new certificate may have the same or different subject public key.
Name Subscriber	A Name Subscriber is an individual (i.e., person) whose name appears as the subject in a certificate. The Name subscriber is tightly coupled with the name certificate in which they are named.
NSS PKI	A Public Key Infrastructure (PKI) for SECRET-high collateral classified networks.
NSS PKI Member Governing Body	The organization established from the participating agencies to assist the PMA and provide governance and oversight to the NSS PKI.
PIV	A physical artifact (e.g., identity card, "smart" card) issued to a government individual that contains stored identity credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation) so that the claimed identity of the cardholder can be verified against the stored credentials by another person (human readable and verifiable) or an automated process (computer readable and verifiable).
PIV-I	A PIV-Interoperable initiative to enable non-federal organizations to issue employee identity cards that are technically interoperable with U.S. government PIV systems, and issued in a manner that allows government and relying parties to trust the cards.
PKI Sponsor	A person who is responsible for the private key associated with a certificate and who asserts that the certificate and associated private key are being used in accordance with this CP.
Policy Management Authority (PMA)	Individual or body established to oversee the creation and update of Certificate Policies, review Certification Practice Statements, review the results of CA audits for policy compliance, evaluate non-domain policies for acceptance within the domain, and generally oversee and manage the PKI certificate policies.
Private Key	A mathematical key (kept secret by the holder) used to create digital signatures and, depending upon the algorithm, to decrypt messages or files encrypted (for confidentiality) with the corresponding public key.
Public Key	A mathematical key that has public availability and that applications use to verify signatures created with its corresponding private key. Depending on the algorithm, public keys can encrypt messages or files that the corresponding private key can then decrypt.
Public Key Infrastructure (PKI)	The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a certificate-based public key cryptographic system. Framework established to issue, maintain, and revoke public key certificates.
Registration Authority (RA)	An entity authorized by the CAS to collect, verify, and submit information provided by potential Subscribers which is to be entered into public key certificates. The term RA refers to hardware, software, and individuals that collectively perform this function.
Registration Authority (RA) Officer	A trusted role, performed by an individual who is responsible for any of the duties of certificate issuance, certificate revocation, or key recovery.

Term	Definition
Registration Practice Statement (RPS)	A document representing a statement of practices an RA employs when performing RA duties for a CAS.
Re-Key	The process of creating a new certificate with a new validity period, serial number, and public key while retaining all other Subscriber information in the original certificate.
Relying Party	An entity that relies on the validity of the binding of the Subscriber's name to a public key to verify or establish the identity and status of an individual, role, or system or device; the integrity of a digitally signed message; the identity of the creator of a message; or confidential communications with the Subscriber.
Renewal	The act or process of extending the validity of the data binding asserted by a public key certificate by issuing a new certificate.
Repository	A trustworthy system for storing and retrieving certificates or other information relevant to certificates. [ABA DSG]
Restoration	The process of changing the status of a suspended (i.e., temporarily invalid) certificate to valid.
Revocation	The process of permanently ending the binding between a certificate and the identity asserted in the certificate from a specified time forward.
Role Subscriber	A Role Subscriber is a role, group, or organization whose name appears as the subject in a certificate.
Root Certification Authority (CA)	The CA that issues the first certificate in a certification chain.
Security Auditor	A trusted role that is responsible for auditing the security of CASs and RAs, including reviewing, maintaining, and archiving audit logs and performing or overseeing internal audits of CASs and RAs.
Security Strength	A number associated with the amount of work (that is, the number of operations) that is required to break a cryptographic algorithm or system. In this policy, security strength is specified in bits and is a specific value from the set {80, 112, 128, 192, 256}. [SP 800-57]
Signature Certificate	A public key certificate that contains a public key intended for verifying digital signatures rather than authenticating, encrypting data, or performing any other cryptographic functions.
Subordinate Certification Authority (CA)	In a hierarchical PKI, a CA whose certificate signing key is certified by another CA, and whose activities are constrained by that other CA.
Subscriber	An entity that (1) is the subject named or identified in a certificate issued to such an entity, and (2) holds a private key that corresponds to a public key listed in that certificate. [ABA DSG]
Suspension	The process of changing the status of a valid certificate to suspended (i.e., temporarily invalid)
System or Device Certificate	A System or Device certificate contains a system or device name as the subject. Examples of systems or devices are workstations, guards, firewalls, routers, web server, database server, and other infrastructure components.
System or Device Subscriber	A System or Device Subscriber is the system or device whose name appears as the subject in a certificate.
Technical Non-Repudiation	The contribution public key mechanisms make to the provision of technical evidence supporting a non-repudiation security service.

Term	Definition
Trusted Agent (TA)	An individual explicitly aligned with one or more RA Officers who has been delegated the authority to perform a portion of the RA functions. A TA does not have privileged access to CAS components to authorize certificate issuance, certificate revocation, or key recovery.