Shared Service Provider Roadmap:
Navigating the Process to Acceptance

Federal PKI Policy Authority
Shared Service Provider Working Group

Version 2.0
March 8, 2007

Document Control Grid

Document Owner	FPKI Shared Service Provider Working Group
Contact	Fpki.webmaster@gsa.gov
Document Title	Shared Service Provider Roadmap

Revision History Table

Date	Version	Description	Author
2/18/04	0.9	Final draft version	Dallas N. Bishoff
2/23/04	1.0	Final release version	Dallas N. Bishoff
2/26/04	N/A	Second draft version	NIST PKI Team
3/1/04	1.1	Second release version	SSP Subcommittee
3/5/04	1.2	Third release version	SSP Subcommittee
1/5/07	2.0	First Revised Draft version	SSP Working Group

1. Executive Summary

The Federal Public Key Infrastructure (PKI) Shared Service Provider (SSP) Program is intended to facilitate outsourcing of PKI services by Federal agencies. The Federal government has established a Certified PKI Shared Service Providers (PKI SSP) List for vendors that have demonstrated the ability to provide managed PKI services that meet government requirements.[1]

This Shared Service Provider Roadmap is intended to identify the background information, phases, and activities related to the selection process for prospective PKI shared service providers. This document identifies the process by which a vendor qualifies for inclusion on the Certified PKI SSP List. It also describes requirements that must be met to maintain certification, as well as contracting considerations.

Questions related to this document should be communicated to fpki.webmaster@gsa.gov for consideration.

1.1. Document Overview

This document is constructed in four sections:

- *Shared Service Provider Overview* describes the components of an SSP and the partitioning of responsibility between the SSP and the contracting agency;
- *Shared Service Provider Requirements* describes the steps that vendors must perform before applying for inclusion on the Certified PKI SSP List. This section identifies the requirements documents that must be considered as part of this process;
- *Application and Acceptance Process* describes the process by which a vendor applies for inclusion on the Certified PKI SSP List and demonstrates that the requirements identified in the preceding section have been satisfied;
- *Post-Acceptance Process* describes the steps a service provider must perform to maintain certification. In addition, the service provider is required to assist contracting agencies in meeting statutory responsibilities and PKI policy requirements. This section also discusses establishing contract vehicles, such as inclusion on a GSA Schedule 70, to simplify government procurement activities.

1.2. SSP Working Group

The Shared Service Provider Working Group (SSPWG) determines the selection criteria, requirements, processes and oversight provisions for selection of Shared Service Providers who will act on the government's behalf under the provisions of the X.509

[1] These requirements have been defined by the Shared Services Provider Working Group, which is a subcommittee of the Federal PKI Policy Authority (FPKIPA). Statutory authority is derived from the E-Government Act, passing from OMB through the Federal CIO Council (http://www.cio.gov/) to the FPKIPA, and in turn to the Shared Service Provider Working Group

Certificate Policy for the U.S. Federal PKI Common Policy Framework (COMMON). The SSPWG is open to, and composed of Federal agency representatives from Federal agencies who are members of the Federal PKI Policy Authority and who are not also Shared Service Providers themselves. Current SSPWG publications can be found at http://www.cio.gov/fpkipa/drilldown_fpkipa.cfm?action=ssp.

2. Shared Service Provider Overview

2.1. SSP Components

The SSP program requires four distinct components: Certification Authority (CA); Repository; Archive; and Registration Authority (RA). While there are many ways to architect, deploy and manage these components, the responsibilities of the components are described below:

- The Certification Authority (CA) issues X.509 certificates and CRLs that comply with COMMON;
- The Repository distributes certificates and CRLs;
- The Archive provides long term secure storage for certificates and CRLs issued by the CA, CA and RA electronic and physical audit logs, audit results, certification and accreditation results, and policy documents; and
- The Registration Authority (RA) performs identity proofing for prospective certificate subjects.

Those shared service providers that support PIV authentication[2] and/or card authentication certificates are also required to deploy an online certificate status protocol (OCSP) server.

The SSP's CA must have a trust relationship with the Common Policy Root CA. This trust relationship may be instantiated by a certificate issued from the Common Policy Root CA to the SSP CA. Where an SSP operates a hierarchy, this relationship may be established indirectly through a certificate issued from the Common Policy Root CA to a superior SSP CA within that hierarchy.

2.2. SSP & Contracting Agency

The SSP program is designed to facilitate outsourcing of PKI services by Federal agencies. Outsourcing PKI services creates responsibilities for both the SSP and the contracting agency; for example, the Registration Authority responsibilities of identity proofing for Federal identity credentials is an agency responsibility. Agencies may contract out RA functions but must maintain responsibility and authority for all decision-making regarding implementation of RA functions and the issuance of credentials.

Responsibilities are divided as follows:

- The SSP provides CA, repository and archive services;
- The SSP develops the Certification Practices Statement covering SSP operations that complies with COMMON;

[2] Note: PIV authentication certificates are mandatory to satisfy HSPD-12/FIPS 201 implementation.

- Optionally, the SSP provides baseline hardware and software to support registration authority operations;[3]
- The SSP obtains the compliance analysis covering SSP-operated components;
- The SSP performs certification and accreditation to satisfy government C&A requirements as specified in OMB Circular A-130, the Federal Information Security Management Act, and NIST Special Publication 800-37;
- The agency is responsible for operating the registration authority component, in compliance with a Registration Practices Statement derived from the CPS;
- The agency is responsible for identifying which agency employees and affiliates are permitted to obtain credentials;
- The agency obtains the compliance analysis covering conformance of RA operations with the RPS; and
- The agency performs a supplemental C&A covering registration-related operations and all relevant activities of the SSP specific to that agency.

3. Shared Service Provider Requirements

3.1. Policy Requirements

This program is intended to result in the issuance of common physical and electronic credentials (a smart card with PKI certificates) for Federal personnel and other authorized users. To ensure these credentials provide sufficient assurance to satisfy most government-wide application and access control requirements, the Shared Service Provider Requirements reflect two core policy documents:

- X.509 Certificate Policy for the Common Policy Framework (COMMON);[COMMON] and
- OMB M-05-024, *Implementation of Homeland Security Presidential Directive 12 – Policy for a Common Identification Standard for Federal Employees and Contractors.*

Service Providers who participate in the SSP program must operate their PKIs in compliance with COMMON. COMMON specifies six distinct certificate policies as follows:

- Software – digital signature and key management certificates for users with software tokens;
- Hardware – digital signature and key management certificates for users with hardware cryptographic tokens;
- Common High Assurance – digital signature and key management certificates issued to users with hardware cryptographic tokens by a PKI operating at the Common High level of assurance;
- Common Authentication – certificates for cardholder identity authentication for PIV card users

[3] Agencies are not required to use the SSP-provided baseline RA solution. An agency may wish to leverage an existing infrastructure by integrating current solutions with the SSP offering.

- Card Authentication – certificates for PIV card validation
- Device – digital signature and key management certificates issued to devices (e.g. web servers)

Providers who operate under the SSP program must implement the Hardware or Common High Assurance policy, or both. All other policies are optional. However, providers who wish to support issuance of PIV cards must also implement the Common Authentication Policy.

Each service provider is required to develop, and operate according to, a Certification Practices Statement (CPS) governing operation of its PKI. The service provider's CPS must be in compliance with COMMON and the following supplemental documents:

- X.509 Certificate and CRL Extensions Profile for the Shared Service Providers Program [PROF];
- Shared Service Provider Repository Service Requirements[REP]; and
- Archive Requirements for Certified PKI Shared Service Providers.[ARCH]

Service Providers are required to obtain a compliance audit[4] from a qualified, independent, third party auditor[5] that establishes:

- The Service Provider's CPS is in compliance with COMMON; and
- The Service Provider's PKI, excluding customer agency responsibilities, is operated in compliance with the CPS. Operational compliance may be determined by a Day Zero Audit, which covers all aspects of the PKI operations except issuance and management of end user certificates.[6]

The compliance auditor is required to complete the Common Policy CPS Evaluation Matrix [CPS EVAL] when evaluating vendor CPS compliance with COMMON.

At a minimum, service providers who operate under the SSP program must support smart cards conforming to SP 800-73. As a consequence, registration authority equipment must support smart card personalization functionality (e.g., PIN reset).

3.2. Various Auditing and Analysis Requirements

There are three distinct audit/analysis requirements an applicant must satisfy in order to become a Certified Shared Service Provider. They are:

1. Completion of CPS Analysis Matrix by independent audit entity using the matrix available on the FPKIPA website. This matrix is used by the SSPWG to evaluate compliance of the applicant's CPS with COMMON.

[4] The Service Provider is responsible for any expenses associated with compliance audits.
[5] The Federal government requires that the compliance auditor be independent and competent in the field. Service Providers may request pre-approval of auditors as a risk management technique.
[6] The Day Zero Audit overcomes the conundrum created by the SSP Program's requirements that the compliance audit be complete before the system is fully deployed and operational. Since the CA has not issued any certificates, the focus is on CA operational and technical security controls.

2. Completion of a "Day Zero" operational compliance audit of vendor's SSP offering. Since the applicant PKI cannot provide production PKI services under COMMON before it is a Certified SSP, it is impossible for an auditor to evaluate whether the applicant is, in fact, operating its SSP PKI in full compliance with COMMON and its own CPS. The auditor can, however, evaluate those elements of the PKI's operations that are in place or are operating in test mode. This is called "Day Zero" compliance and a detailed discussion of the contents of this audit may be found on the FPKIPA website.
3. Completion of Certification and Accreditation for Federal IT Systems, a security-focused systems audit required by OMB A-130 Appendix III and comprising a full assessment of the architecture, operations and documentation of– in this case – the applicant SSP PKI, based on FIPS 199 Moderate Impact Level and NIST SP 800-53. This audit may be performed by the same independent entity that performs the other audit and analysis work or by a different entity. The certification process will create a reusable C&A report that applies equally to all Federal agencies contracting with that particular SSP. See GSA Memorandum of December 6 2006, *Recognition of Certification and Accreditation of Certified PKI Shared Service Providers Across Agency Boundaries*. Note that certification and accreditation is performed at the Service Provider's expense.

As previously noted, in addition to these activities, the Agency PKI eventually supported by the Certified SSP must also operate a Registration Authority in accordance with a defined set of Registration Practices. The Registration Practices cover procedures instituted by the customer Agency for registration services, and must comply with the Common Policy elements that address registration services and functions. The SSP supporting the Agency is responsible for working with its customer to ensure that the registration practices fit smoothly within the overall CPS package and satisfies COMMON on relevant points. The registration practices must also be audited by an independent, third party auditor and the results included in the documentation package for the Agency PKI.

Finally, the SSP and Agency have ongoing audit and analysis responsibilities to ensure that the PKI continues to operate at the appropriate level of trustworthiness. The Service Provider must perform an annual audit of its implementation of the Agency PKI in accordance with the requirements of COMMON. This annual audit will include the operational registration elements. Also, OMB A-130 Appendix III requires that the system perform a triennial Certification and Accreditation. At a minimum, operational registration elements must be evaluated based on FIPS 199 Moderate Impact Level.

Successful completion of the PKI audit satisfies many of the requirements of the triennial C&A and may be used as input to the C&A process. The FPKIPA has analyzed the SP 800-53 moderate baseline and determined that a SSP PKI audit addresses many of the required controls.

4. Application and Acceptance Process

This section outlines the steps an applicant is required to follow to be accepted for inclusion on the Certified PKI SSP List.

4.1. Initial Application

The SSP applicant shall submit a written request to the SSPWG via fpki.webmaster@gsa.gov. The request shall be accompanied, at a minimum, by the following documents:

- A narrative description of the components for the proposed system, which may include an architectural diagram of the proposed PKI implementation. This description should include an explanation of the proposed division of responsibilities between the SSP and contracting agencies.
- A letter from the compliance auditor indicating that the applicant CPS is in compliance with COMMON and the applicant is operating the CA in compliance with their CPS. In doing so, the letter should address the following points:
  a. Identify the individuals performing the audit
  b. Identify the experience these individuals have in auditing PKI systems
  c. Describe the relationship between the auditor and the SSP (outside auditor, Inspector General Office of Audits, etc.)
  d. Indicate date the audit was performed
  e. Describe methodology used for determining operations compliance (e.g. Day Zero Audit)
  f. Identify the documents reviewed (including version and date)
  g. Assert that the CPS has not changed since the previous review OR a statement indicating the revised SSP CPS continues to conform to the requirements of the Common Policy
  h. Assert that the SSP CA is operating in conformance to the requirements of the SSP CPS.
- The applicant CPS;
- The completed CPS Evaluation Matrix
- A plan for completing the System Certification and Accreditation

.

It is also recommended that any supporting documentation or relevant extracts from supporting documents cited in the CPS be submitted as part of the package.

- Optionally, the Application Package may also include a System Certification and Accreditation (C&A) package for review and approval by the Authorizing Official. If included, the System C&A package must include the following:
  a. System Security Plan
  b. Security Assessment Report
  c. Plan of Action and Milestones
  d. Contingency Plan
  e. Contingency Plan Test Report
  f. Risk Assessment Report

Note that these documents are not required to initiate the process, but must be reviewed and approved before a Service Provider can be placed on the Certified PKI SSP List. (See Section 4.3, below) Submitting these documents at initial application may help to expedite the approval process.

A checklist, "Application for Inclusion on the Certified PKI Shared Service Providers List", is available at http://www.cio.gov/fpkipa/documents/SSPapplication.pdf to assist in completing the application process.

4.2. CPS Analysis Matrix Review

Once the SSPWG has received the application package and verified the presence of the required documentation, the SSPWG will conduct a review of the CPS Analysis Matrix. The responses provided by the auditor will be assessed to ensure they satisfy the requirements of COMMON. Questions or concerns that cannot be answered by consulting the supporting documentation provided with the matrix will be referred back to the applicant for resolution. If necessary, the SSPWG will invite the applicant to a meeting to resolve open issues. In some cases, the applicant may be asked to provide copies of additional documents cited in the CPS, where these are considered critical to resolving particular issues or concerns. This is an iterative process and may be repeated several times before successful completion. Once the review has been completed successfully, the SSPWG will schedule the Operational Capabilities Demonstration (OCD).

4.3. Operational Capabilities Demonstration

Upon successful completion of the CPS Evaluation Matrix review, the SSPWG will contact the SSP candidate to arrange for an Operational Capabilities Demonstration (OCD).

The OCD is the process by which the government validates the ability of an SSP candidate to operate a PKI environment that is compliant with COMMON and the supplemental documents specified in Section 3.1. The "Operational Capabilities Demonstration Criteria for PKI Shared Service Provider Candidates" specifies the functionality to be demonstrated during the OCD. [OCD] See http://www.cio.gov/fpkipa/documents/OCDcriteria.pdf.

The SSP OCD shall be approved if the government determines that all OCD criteria were successfully demonstrated.

If the government determines that criteria in the OCD were not successfully demonstrated, the applicant will be provided with a list of criteria that were not met. Depending upon the severity of the issues, the government may choose from the following options:

- If the issues are judged to be minor, the SSPWG may accept a written attestation that the issues have been corrected and approve the OCD; or

- The SSPWG may require that the vendor perform a new OCD.

If remediation requires a change to the CPS, the government will require an update to the compliance audit.

4.4. Government Review of Audit Documentation

The audit letter covering SSP operations and the Certification package is reviewed to ensure the security requirements of the Federal PKI and the Federal Information Security Management Act are being satisfied. See Section 3.2 for additional information concerning the various Audit requirements.

Note that the C&A may be performed in parallel with the OCD if the Certification package is included in the initial application.

4.4.1. Compliance Analysis

The SSPWG will review the compliance analysis letter to ensure the requirements identified in Section 4.1 are addressed satisfactorily. The SSPWG may approve the compliance analysis letter, reject the compliance analysis letter, or ask for further clarifications. The SSPWG Chair will prepare a letter to the applicant indicating the decision of the SSPWG and any corrective action required. If the compliance analysis letter is accepted, the SSP applicant will be notified that it has achieved standing as a Certified PKI Shared Service Provider. Certified PKI SSPs must complete a successful Certification and Accreditation review conducted by GSA on behalf of the Federal community prior to entering production operational status with an agency customer.

4.4.2. Certification and Accreditation

The government's Designated Approving Authority (DAA) will review the submitted System Certification and Accreditation package described in Section 4.1 above. Review will be conducted only if the full package has been submitted. The documentation must cover the SSP operated core components including any SSP-supplied RA hardware and software. If necessary, the Information Systems Security Manager will meet with the applicant to resolve residual issues. Once the C&A is successfully completed, the DAA will authorize the system to process government data. In the event security issues cannot be resolved, the DAA will deny authority to operate and the SSP approval will be revoked.

4.5. Certified PKI SSP List

Upon successful completion and approval of the CPS Analysis Matrix Review (Section 4.2), the OCD (see Section 4.3), and the compliance audit letter review (see Section 4.4.1), the SSPWG shall add the applicant to the Certified PKI SSP List. Upon completion of the C&A, the list is updated with a link to the document granting "Authority to Operate."

5. Post-Acceptance Process

5.1. Contract Execution Activities

Once fully approved, companies on the Certified PKI SSP List are invited to submit proposals for Special Item Number (SIN) 132-61, Public Key Infrastructure (PKI) Shared Service Providers (PKI SSP) Program, on the Group 70 Schedule. Those companies already participating on Group 70 Schedule should also apply to SIN 132-61.

Certified PKI SSPs are encouraged to include additional services in contract vehicles. Examples include:

- Custom integration activities to support integrating the SSP with agency owned equipment and PKI-enabling agency applications;
- RA and end user training; and
- Policy development services for agencies that maintain an agency-specific Registration Practices Statement (RPS). See [RA REQ] for details regarding the contents of an RPS.

5.2. Recurring Activities

5.2.1. Yearly Compliance Audits

COMMON mandates yearly compliance audits performed by a competent, independent third party.

The SSP shall submit a compliance analysis letter each year covering SSP-operated components for as long as they continue as Certified SSPs. Compliance analyses shall be processed as in Section 4.4.1 and must address the elements listed in Section 4.1. If an SSP is determined to be out of compliance, it shall submit a remediation plan to the SSPWG for consideration. Failure to submit an annual compliance audit letter, or findings that indicate the SSP is out of compliance with COMMON, may result in removal from the Certified PKI SSP List. Failure to comply with requirements will result in revocation of the SSP COMMON digital certificate and notification to customer agencies.

5.2.2. Certification and Accreditation Maintenance Process

OMB A-130 requires that the certification and accreditation process be repeated every three years, or whenever there is a major modification to the system. Therefore, the SSPs are required to submit System Certification and Accreditation packages on a triennial basis, at a minimum. In the event it is determined that major changes to the SSP PKI services have occurred, a new full C&A or partial (delta) C&A may be required.

5.3. Non-Compliance Procedures

The SSPWG will continue to monitor the Certified SSPs for compliance, primarily through the annual audits and on-going C&A activities, but also in response to Federal

agency questions or complaints. If the SSPWG believes an SSP is not compliant, before formal action is taken, the SSPWG will attempt to resolve the issue informally. If the matter cannot be resolved informally within 14 days from initial notification, the SSPWG will issue a show-cause letter (SSP will have to respond and show-cause why they should not be canceled out of the program). The show-cause letter will identify the issue and provide instruction to the SSP concerning resolution/next steps. Failure to respond to the show-cause notice within 14 days, in and of itself, is grounds for removal from the Certified PKI Shared Service Provider List and suspension of Schedule 70, SIN 132-61 participation.

5.4. SSP - Agency Interaction

5.4.1. Agency Audit

Each agency that obtains services from an SSP is responsible for ensuring its Registration activities comply with COMMON and the requirements of the SSP CPS. Therefore, each agency should provide a copy of its registration practices to the SSP. The SSP must provide the Agency with sufficient information regarding SSP-provided equipment to facilitate this process. The registration practices are subject to FISMA compliance review.[7]

5.4.2. Agency System Accreditation

Each agency is responsible for the C&A of any agency information system that interconnects with a Certified PKI SSP. The accreditation boundary of the agency information system does not include the Certified PKI SSP information system. The GSA C&A can be accepted by each agency utilizing a Certified PKI SSP as assurance that the risk to the agencies' operations, assets, and to individuals arising from the use of the Certified PKI SSP is at an acceptable level of risk in accordance with NIST Special Publication 800-53 guidance on the use of external information system services and service providers.

5.4.3. Policy Coordination

In the event COMMON is revised, the Certified PKI SSPs will be advised and provided an opportunity to comment during the revision process. Once the revisions have been published and reach the effective date, the SSPs must be in compliance with the new version of COMMON or risk suspension or revocation of certified status. Consultation and coordination with Agency customers may be necessary if revisions affect registration authority functions.

5.4.4. Agency Archive Requirements

The agency is responsible for (1) developing a records management plan that will meet its regulatory, legal and business needs as well as the SSP archive requirements [ARCH],

[7] For FIPS-201 compliance, NIST Special Publication 800-79, *Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations,* applies to agency registration practices.

(2) obtaining NARA approval of its plan, (3) conveying that plan's archival requirements to the SSP, and (4) assuring that the SSP is capable of fulfilling those agency requirements and understands its obligation as an SSP to do so.

6. Glossary

Access Control	Process of granting access to information system resources only to authorized users, programs, processes, or other systems. [NS4009]
Accreditation	Formal declaration by a Designated Approving Authority that an Information System is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. [NS4009]
Applicant	Any organization seeking to participate in the Federal Certified PKI Shared Service Provider program.
Archive	Long-term, physically separate storage.
Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures. [NS4009]
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. [NS4009]
Certificate	A digital representation of information which at least (1) identifies the certification authority issuing it, (2) names or identifies its user, (3) contains the user's public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it. [ABADSG].
Certification Authority (CA)	An authority trusted by one or more users to issue and manage X.509 public key certificates and CRLs.
Certificate Policy (CP)	A certificate policy is a specialized form of administrative policy tuned to electronic transactions performed during certificate management. A certificate policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery and administration of digital certificates. Indirectly, a certificate policy can also govern the transactions conducted using a communications system protected by a certificate-based security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications.
Certification and Accreditation (C&A)	Comprehensive evaluation of the technical and non-technical security features of an IT system and other safeguards, resulting in accreditation, to establish the extent that a particular design and implementation meets a set of specified security requirements. Federal requirements for C&A are established by NIST SP 800-37 and SP 800-53.

Certification Practice Statement (CPS)	A statement of the practices that a CA employs in issuing, suspending, revoking, and renewing certificates and providing access to them, in accordance with specific requirements (i.e., requirements specified in this CP, or requirements specified in a contract for services).
Certificate Revocation List (CRL)	A list maintained by a certification authority of the certificates that it has issued that are revoked prior to their stated expiration date.
Certified PKI Shared Service Providers	Providers of PKI Services that have successfully completed the review and evaluation activities described in this Roadmap.
Common Policy Framework (COMMON)	Set of policies specifically designed for the U.S. Federal government's deployment and use of public key technology.
Compliance Analysis	Independent review of documentation and operations to ensure the systems are operated in accordance with their governing documentation.
Day Zero Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, on the core PKI Service Offering. This review does not include the operational aspects associated with the issuance of credentials to end users since these operations have not been initiated at the time of the Day Zero Audit.
Digital Signature	The result of a transformation of a message by means of a cryptographic system using keys such that a relying party can determine: (1) whether the transformation was created using the private key that corresponds to the public key in the signer's digital certificate; and (2) whether the message has been altered since the transformation was made.
Federal Public Key Infrastructure Policy Authority (FPKIPA)	The FPKIPA is a Federal Government body responsible for setting, implementing, and administering policy decisions regarding the Federal PKI Architecture.
Online Certificate Status Protocol (OCSP)	An Internet protocol used for obtaining the revocation status of an X.509 digital certificate.
Operational Capabilities Demonstration (OCD)	Evaluation process to determine the ability of the applicant service to perform a set of prescribed functions.
Personal Identity Verification (PIV)	Term referring to the HSPD-12-compliant identity credential issued to all Federal employees and select Federal contractors.
Public Key Infrastructure (PKI)	A set of policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public/private key pairs, including the ability to issue, maintain, and revoke public key certificates.
Registration Authority (RA)	An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., a registration authority is delegated certain tasks on behalf of an authorized CA).
Repository	A database containing information and data relating to certificates as specified in this CP; may also be referred to as a directory.

Risk	An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.
Root CA	In a hierarchical PKI, the CA whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain.
Server	A system component that provides a service in response to requests from clients.
Shared Service Provider	Any organization that provides like-services to multiple customers.
Shared Service Provider Working Group (SSPWG)	A working group of the Federal PKI Policy Authority charged with evaluating the documentation submitted by applicants and conducting Operational Capabilities Demonstrations to determine eligibility for participation in the Certified PKI Shared Service Provider program.
Smart Card	Any pocket-sized card with embedded integrated circuits that allows storage and retrieval of information. For the purposes of this document, a smart card is a dual-interface card, allowing both contact and contactless access to a microprocessor that contains, among other features a cryptographic engine capable of generating strong asymmetric key pairs.

7. References

[800-37] NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, Draft Version 2 June 2003. Available at <http://csrc.nist.gov/publications/drafts/sp800-37-Draftver2.pdf>

[A-130] Office of Management and Budget Circular A-130, Revised (Transmittal 4). Available at <http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html>

[AUDIT] *Audit Standards for Certified PKI Shared Service Providers*, 29 January 2007. Available at <http://www.cio.gov/fpkipa/documents/AuditStandards.pdf>

[ARCH] *Archive Requirements For Certified PKI Shared Service Providers*, 29 January 2007. Available at <http://www.cio.gov/fpkipa/documents/ArchiveRqmtsForSSP.pdf>

[COMMON] *X.509 Certificate Policy for the Common Policy Framework*, v2.5, 16 October 2006. Available at <http://www.cio.gov/fpkipa/documents/CommonPolicy.pdf>

[CPS EVAL] *CPS Evaluation Matrix For Evaluation Against the Requirements for the Common Policy Framework, Version 1.5*, 23 October 2006. Available at <http://www.cio.gov/fpkipa/documents/CPSmatrix.doc>

[FISMA] *Federal Information Security Management Act of 2002 (Title III of E-Gov)*, Available at <http://csrc.nist.gov/policies/FISMA-final.pdf>

[GSC-IS] NISTIR 6887 *Government Smart Card Interoperability Specification (GCS-IS) Version 2.1*. Available at <http://csrc.nist.gov/publications/nistir/nistir-6887.pdf>

[OCD] *Operational Capabilities Demonstration Criteria for PKI Shared Service Provider Candidates*, 29 January 2007. Available at <http://www.cio.gov/fpkipa/documents/OCDcriteria.pdf>

[PROF] *X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Providers (SSP) Program*, 6 February 2006. Available at <http://www.cio.gov/fpkipa/documents/CertCRLprofileForCP.pdf>

[RA REQ] *Registration Authority (RA) Requirements*, 29 January 2007. Available at <http://www.cio.gov/fpkipa/documents/RArequirements.pdf>

[REP] *Repository Service Requirements*, 29 January 2007. Available at <http://www.cio.gov/fpkipa/documents/SSPrepositoryRqmts.pdf>