GSA PKI
Shared Service Provider
Program Guide

[June 30, 2023]

DRAFT / PRE-DECISIONAL

Revision History

Date	Version	Description	Author
02/14/2023	1.0	Initial draft	SSP PMO

Table of Contents

Overview

The General Services Administration (GSA), Office of Government-wide Policy, manages the Public Key Infrastructure (PKI) Shared Services Provider (SSP) program. The primary program focus is to help agencies meet the policy intent of Homeland Security Presidential Directive 12, as well as achieve digital signature interoperability.

A GSA PKI SSP is a commercial PKI provider who has completed Federal PKI compliance activities to receive a certification authority certificate and is listed on the GSA Multiple Award Schedule. This document is reviewed annually and has three major sections:

- Section 1 - Outlines GSA management and acquisition controls of the PKI SSP Program.
- Section 2 - Defines the application and ongoing maintenance process to apply and stay in the GSA PKI SSP Program.
- Section 3 - Lists available services that a SSP should offer.

Audience

This document is primarily for the following audience: :

1. Commercial PKI vendors who are interested in becoming a GSA PKI SSP.
2. Existing GSA PKI SSP Program members to refresh their knowledge of ongoing maintenance requirements.
3. Federal agency customers who want to understand the GSA PKI SSP program or find contact information for the program management.

If you have questions about this document or the outlined process, contact GSAPKISSP@gsa.gov.

Section I: GSA PKI SSP Program

The GSA SSP Program has a long history of successfully providing digital certificate services for employees, contractors, and affiliates. The program was started in December 2004 when the Office of Management and Budget (OMB) issued a directive, M-05-05, directing federal agencies to buy their digital certificate services through the SSP Program. Almost 20 years later, the program is a cornerstone for some federal agencies despite the drive to expand new services in a thin market.

In 2019, a new OMB directive, M-19-17, was released that requires shared services such as the SSP Program be updated to enable strong government oversight. In response to this directive, GSA is strengthening its oversight by establishing a framework among its Managing Partners and with approved SSPs. The framework is a Memorandum of Agreement (MOA) that provides clarity of intent and high-level responsibilities and accountability.

Who Is a GSA PKI Shared Service Provider?

A GSA PKI Shared Service Provider is a commercial PKI vendor who has a signed MOA with the GSA PKI SSP Program Office and is listed on the GSA PKI SSP Multiple Award Schedule.

If a vendor fails to be added to the Multiple Award Schedule, GSA will rescind the Authorization to Operate and the Federal Public Key Infrastructure Policy Authority (FPKIPA) will revoke the certification authority certificate.

Should My Company Apply to the Program?

There are multiple advantages to becoming a GSA PKI SSP. They are as follows:

- You will leverage your existing PKI platform to also offer federal PKI certificates.
- Your Federal Government customers will want to procure your services with a GSA Multiple Award Schedule.
- You will expand your federal customer footprint by marketing your service through the GSA Multiple Award Schedule (MAS).

In making a business decision to join the SSP Program, it is important to understand what resources are needed to prepare for and keep your information systems in a good security posture.

Who Manages the GSA PKI SSP Program?

The SSP Program is managed by the GSA Office of Government-wide Policy, Office of Technology Policy, Identity Assurance and Trusted Access Division as the Program Office. Other offices within GSA support the Program Office as well.

GSA Office of Technology Policy

The SSP Program Office oversees and guides the business and security practices necessary for SSPs to provide digital certificate services to federal agencies. Responsibilities include internal and external coordination for integrating and synchronizing program activities. They are as follows:

- Internally, the SSP Program Office meets with its GSA counterparts to ensure services are secure and available through the proper contract vehicle.
- Externally, the office meets with federal agencies and SSPs to learn about successes and how processes and service delivery can be improved.

The GSA, Associate Deputy Administrator in the Office of Government-wide Policy, Office of Technology is the Authorizing Official of GSA PKI SSP vendor systems and is ultimately responsible for their secure operation. The GSA PKI SSP Program Office and Program Manager reside in the Identity Assurance and Trusted Access Division within the Office of Technology Policy. The GSA PKI SSP Program Manager has the following responsibilities:

- Direct and coordinate activities between the GSA PKI SSPs, the Federal PKI Policy Authority and GSA supporting offices, Office of the Chief Information Security Officer, and the Federal Acquisitions Service.
- Coordinate customer interest meetings to understand customer needs and challenges, plan service enhancements, and remediate issues.
- Invite and coordinate customer agency participation in GSA A&A security meetings.
- Brief interested parties on the latest program activities.
- Regularly report the latest program activity to the Authorizing Official and the Identity Assurance and Trusted Access Division Director.

GSA Office of Chief Information Security Officer

The GSA, Office of Chief Information Security Officer (OCISO) provides security policies and guidance so SSPs can implement security controls in their information systems to guard against cyber-attacks. The security team in the OCISO receives a Security Assessment Report (SAR) from the SSP to review the results of the security control assessment for the authorizing official and system owner. Based on the review, the OCISO makes a recommendation to the GSA Authorizing Official on whether to grant an Authorization to Operate (ATO) to a SSP. The decision is formalized in an ATO letter and provided to the GSA PKI SSP. The OCISO is also responsible for overseeing risk management activities with the GSA PKI SSP.

GSA Federal Acquisition Service

The GSA Federal Acquisition Service (FAS) connects government buyers with the GSA PKI SSPs. The FAS organization captures the GSA PKI SSP services and sets prices, terms, and conditions of the Special Item Number (SIN) on the GSA Multiple Award Schedule. The SSP SIN is intended to make it easier for potential buyers to search for the digital certificate services offered by the GSA PKI SSPs.

Section II: SSP Application and Maintenance Activities

Federal agencies requiring digital certificate services from a SSP will send a Request for Quotation or a Request for Proposal based on the SSP SIN — sending alerts to SSPs. Federal agencies can expect a response from the SSPs that reflects the due diligence completed by the Federal Acquisition Service (FAS) to offer SSPs that satisfy federal requirements.

Federal agencies' participation in the SSP Program is important. While their purchases through the program help drive revenue, their ultimate participation leads to the Federal Government's way of using trusted SSPs to issue and manage digital certificates for devices, federal employees, contractors, and other affiliated personnel. Additionally, federal agencies using the program will leverage the SSPs' infrastructure components for digital certificate services, which can result in cost savings derived from economies of scale through large volume of certificate purchases.

Federal agencies have the opportunity to share in the risk management activities by providing their security controls or hybrid security controls to GSA for them to populate into a SSP's security posture for a holistic view. This will help focus on the whole PKI solution rather than focus on the PKI infrastructure. Federal agencies are encouraged to participate in the security meetings with their SSP to jointly address problems related to risk.

Application Process

There are five major steps to apply to become a GSA PKI SSP. They are as follows:

- Initiate an application with the GSA PKI SSP Program Office and sign the GSA PKI SSP MOA.
- Complete PKI pre-conditions and submit to the FPKIPA through the GSA PKI SSP Program Office for verification.
- Complete the federal PKI certification process and send an executive copy of the FPKIPA MOA to the GSA PKI SSP Program Office.
- Complete GSA Security Assessment & Authorization (SA&A) activity and receive an ATO.

- Apply to the GSA MAS and, after acceptance, the vendor is added to idmanagement.gov government identity trust services and officially listed as a GSA PKI SSP.

Step 1 - Initiate an Application and Sign GSA PKI SSP MOA

The GSA establishes a MOA with a GSA PKI SSP to communicate the mutually accepted actions of all parties involved in the agreement. The MOA indicates the parties in the agreement have reached an understanding of their roles and responsibilities and are moving forward with the acceptance of the SSP participating in the program. See Appendix A for a sample MOA.

A PKI Vendor will be asked for proof or to provide attestations regarding their systems and technical capabilities. Other pre-conditions may be applied as necessary, such as past performance, degree of experience, organizational maturity, and ability to scale operations to meet expected long-term demand and the rigors in completing the Federal PKI certification process.

MOA Procedural Guidance:

- Send an email to GSAPKISSP@gsa.gov requesting admission to the GSA PKI SSP Program.
- SSPs must obtain, review, and sign the MOA from the SSP Program Office.

Once an MOA is signed, the GSA PKI SSP will sponsor the vendor to apply to the Federal PKI Policy Authority.

Step 2 - Complete PKI Pre-Conditions

A prospective GSA PKI SSP must meet the following basic pre-conditions as outlined in the X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework [COMMON CP] to demonstrate readiness for the PKI certification process.

1. Provide Certification Authority (CA), repository, and archive services. The PKI Vendor must operate a self-signed CA instead of relying on a certificate issued from the Federal Common Policy CA. This ensures that if there is an issue with the GSA PKI SSP, the Federal PKI can revoke the certificate from the Federal Common Policy CA without impacting the GSA PKI SSP customer certificates.
2. Develop and maintain a Certification Practice Statement (CPS) covering PKI operations that comply with [COMMON CP] and issue certificates according to

the Common Policy X.509 Certificate and Certificate Revocation List (CRL) profiles.

3. Work with its customers to ensure registration practices fit smoothly within its overall CPS package and comply with [COMMON CP].
4. Implement all applicable PIV-related policies, such as common-authentication, common-cardAuth, and common-piv-contentSigning.
5. Ensure it understands and can fulfill its customers' archive requirements and understands its obligation to do so.
6. Collaborate and exchange information and documents as necessary with any other party performing the Registration Authority (RA) duties.
7. Support federal agency customer audits and assessments as requested.
8. [Optionally] Provide baseline hardware and software to support RA operations.

Any changes to these pre-conditions will be coordinated through the GSA SSP Program Office, which can amend the conditions any time to ensure the best interests of the Federal Government are met. Once the GSA PKI SSP verifies the pre-conditions, the vendor submits this information to the Federal PKI Policy Authority to begin the Federal PKI Certification process.

Step 3 - Apply for Federal PKI Certification

The PKI Vendor must successfully meet five compliance and conformance activities with the FPKIPA:

- Sign a memorandum of agreement with the FPKIPA.
- Document conformance with the [COMMON CP], which measures the degree to which the PKI Provider's CPS conforms with [COMMON CP].
- Perform a Day Zero Audit to ensure the applicant's PKI is operating in conformance with applicable [COMMON CP] requirements.
- Demonstrate PKI operational capabilities, which validates the PKI Provider's ability to operate a PKI compliant with [COMMON CP] and other relevant operating documents.
- Obtain an ATO for its PKI system through GSA, which establishes the extent to which the Applicant's PKI meets security and privacy requirements defined by the organization, government guidelines, and federal mandates. Findings are documented in a formal authorization package that informs the ATO decision. The ATO is conditional upon the PKI vendor successfully applying to and getting on the GSA PKI SSP MAS.

If the Federal PKI Policy Authority approves the PKI vendor, both parties execute an MOA to establish roles, responsibilities, and requirements in maintaining the Federal PKI certification.

Federal PKI Certification Guidance:

- The GSA PKI SSP Program Office will coordinate PKI vendor information needs with the GSA supporting offices.
- The PKI vendor shares an executed copy of the Federal PKI Policy Authority MOA with the GSA PKI SSP Program Office.

After an executed Federal PKI Policy Authority MOA is shared with the GSA PKI SSP Program Office, GSA can verify security activities to issue an ATO.

Step 4 - Receive an Authorization to Operate

A Security Assessment & Authorization (SA&A) at the moderate impact level must be performed on the SSP's information system by a third-party auditor. Performing an SA&A satisfies government requirements as specified in the Federal Information Security Modernization Act 2014 (FISMA 2014) and other associated documents. An SA&A includes three components — a security assessment, a resulting security authorization, and continuous monitoring.

The Security Assessment determines that selected controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security and privacy requirements for the system and the organization.

The Security Authorization provides organizational accountability by requiring a senior management official to determine if the security and privacy risk to organizational operations and assets, individuals, and other organizations (if applicable) is acceptable. The security team within the GSA, OCISO reviews the SAR along with applicable security documents to recommend a Security Authorization to the GSA senior management official in the SSP Program Office.

Security Assessment & Authorization Procedural Guidance:

- Engage an Assessor or Assessment Team that is an independent third-party competent in Public Key technology.
- Format System Security Plan in Open Source Control Assessment Language.

- Obtain all necessary GSA SA&A guidance documents and security artifact templates from the security team in the GSA Office of Chief Information Office. Documents to be obtained and used include:
    - **Managing Enterprise Risk** — GSA policy detailing annual documentation requirements.
    - **SA&A Artifact Templates** — Examples include Incident Response template, System Security Plan template, Penetration Testing and Results template, Plan of Action and Milestones (POA&M) template, and Security Assessment Report template.
    - **FPKI 800-53 Overlay (OVERLAY)** — Details security controls applicable to SSP PKI systems and provides supplemental guidance on additional requirements for those controls and enhancements.
- Perform the Assessment, completing all provided templates and guidance.
- Develop a Plan of Action and Milestones (POA&M) to facilitate remediation of any security findings.
- Provide the Assessment Package to the OCISO's Information Systems Security Manager (ISSM), who reviews the package to ensure FISMA security requirements are met.
- The Information System Security Management (ISSM) on the security team creates an authorization package and submits it to the Authorizing Official (AO) in the SSP Program Office.
- The AO makes a risk determination that reflects the risk management strategy, including risk tolerance. Responses and mitigations for identified risks are provided by the ISSM.
- The AO decides whether to approve or deny authorization to operate.
- If approved, the AO signs and issues an ATO.
- The SSP performs risk management activities documented in the IT Security Procedural Guide: *Managing Enterprise Cybersecurity Risk CIO-IT Security-06-30* and the *SSP Handbook*.

NOTE: The ATO is not a governmentwide risk acceptance. Each federal agency must issue an ATO for its own use of the SSP services and review continuous monitoring deliverables to ensure the security posture remains sufficient for their continued use.

To avoid significant delays, a SSP should not use their own versions of SA&A-related documents or templates. It is important for the SSP to consider the resources needed for ongoing risk management activities.

Once a vendor receives an ATO, they apply to the GSA Multiple Award Schedule to complete the process and be recognized as a GSA PKI SSP.

Step 5 - Apply to GSA MAS and Get Listed as an Identity Trusted Service

Upon receiving an ATO and being confirmed as a GSA PKI SSP, the vendor is ready to apply to the GSA MAS to offer digital certificate services governmentwide. The schedule provides a customer agency with a level of assurance that the SSP has been pre-vetted and is offering the best value. Once a SSP is on a schedule, it affords them access to other GSA schedule opportunities.

Acquisition Procedural Guidance:

- Submit an Information Technology Package for GSA Special Item Number (SIN) 541519PKI on the GSA MAS. For assistance, please visit the GSA's website: https://www.gsa.gov/buy-through-us/purchasing-programs/gsa-multiple-award-schedule/mas-roadmap

- Collaborate with the FAS to clarify or supplement the package for contract determination.

NOTE: If the OCISO and SSP Program Office believe the SAR will be favorable based on preliminary reviews and discussions, the SSP does not have to wait for the ATO letter to submit an Information Technology Package to FAS. These efforts can be worked in parallel to offer digital certificate services on the day of receiving the ATO letter.

After the vendor is listed on the GSA MAS, the vendor submits a business and technical point of contact to the GSA PKI SSP Program Office. This information is publicly posted on idmanagement.gov under Government Identity Trust Services to identify the vendor as a GSA PKI SSP and assist agencies in identifying federally-compliant PKI services. GSA will market the Multiple Award Schedule and vendors listed on it as the premier vehicle for Federal Government agencies to acquire federally-compliant PKI services.

Maintenance Activities

A GSA PKI SSP must complete ongoing maintenance activity to remain in the program. If these maintenance activities are not completed, the vendor may lose either its Authorization to Operate or Federal PKI certification.

PKI Maintenance

A GSA PKI SSP must comply with all federal PKI-directed activities by:

1. Completing annual PKI compliance activities as outlined in the Federal PKI Annual Review requirements.
2. Following the FPKI Incident Management Plan in the event of a PKI-related incident.

SA&A Maintenance

The GSA PKI SSP Program Office and GSA's security team perform continuous monitoring, annual checks, monthly scanning, vulnerability management, and other risk management strategies to maintain operational status. Risk management activities are documented in the IT Security Procedural Guide: Managing Enterprise Cybersecurity Risk CIO-IT Security-06-30 and the SSP Handbook.

GSA PKI SSP MAS Contract Maintenance

The vendor must maintain its GSA PKI SSP MAS Contract to stay in compliance with the GSA PKI SSP MOA. If a vendor cannot maintain a GSA PKI SSP MAS Contract, the PKI vendor will coordinate decommission activity through the GSA PKI SSP Program Office with customer agencies, the Federal PKI Policy Authority, and supporting GSA offices.

Section III: Digital Certificate Services

While the SSP Program has primarily focused on digital certificates for Personal Identity Verification (PIV) cards, the [COMMON CP] provides opportunities (and supporting Object Identifiers (OIDs) for SSPs to offer additional services to federal agencies.

Current Services

PIV Certificates

A PIV card is a hardware-based smart card that conforms to Federal Information Processing Standard 201. It contains five digital certificates of which four are available to the user. A PIV card is issued to either a federal employee or contractor who has a favorably-adjudicated Tier 1 or higher federal background investigation. PIV certificates issuance is contingent on the agency customer operating a card management system.

Type	COMMON OID
Certificates for authentication to logically and physically access federal assets	id-fpki-common-authentication
Certificates for encrypted email	id-fpki-common-policy OR id-fpki-common-hardware
Certificates to digitally sign emails and documents	id-fpki-common-hardware
Certificates for Card Authentication	id-fpki-common-cardAuth
Certificates used by a Card Management System to digitally sign content embedded in PIV cards	id-fpki-common-pivcontentSigning

Derived PIV Certificates

A derived PIV certificate is either a software or hardware certificate issued when the user demonstrates ownership of a PIV card. A derived PIV certificate is issued to a mobile device or other form factors such as FIDO USB security keys and device Trusted Platform Module. A derived PIV certificate is issued and used where it is difficult to leverage a smart card form factor such as on devices or platforms that cannot use a smart card reader.

Type	COMMON OID
Derived-PIV authentication certificates for use on mobile devices or other form factors such as FIDO USB security keys and Trusted Platform Modules	id-fpki-common-derived-pivAuth-hardware or id-fpki-common-derived-pivAuth

Derived PIV signature certificates for use on mobile devices or other form factors such as FIDO USB security keys and Trusted Platform Modules	id-fpki-common-policy, id-fpki-common-hardware, or id-fpki-common-high
Derived PIV encryption certificates for use on mobile devices or other form factors such as FIDO USB security keys and Trusted Platform Modules	id-fpki-common-policy, id-fpki-common-hardware, or id-fpki-common-high

PIV-I Certificates

PIV Interoperable(PIV-I) is a hardware-based smart card that follows the same technical standard as the PIV card, can interoperate with the PIV infrastructure, but does not require a favorably adjudicated Tier 1 or higher federal background investigation. A PIV-I card is issued to individuals who do not qualify for a PIV card. See the PIV-I playbook for more details.

Type	**COMMON OID**
PIV Interoperable authentication certificates	id-fpki-common-pivi-authentication
PIV Interoperable digital signature certificates	id-fpki-common-policy, id-fpki-common-hardware, or id-fpki-common-high
PIV Interoperable encryption certificates	id-fpki-common-policy, id-fpki-common-hardware, or id-fpki-common-high
PIV Interoperable card authentication certificates	id-fpki-common-pivi-cardAuth
PIV Interoperable content signing certificates	id-fpki-common-pivi-contentSigning

Device Certificates

Device certificates can be issued to devices such as domain controllers, web sites, servers, or other types of devices on which they want to establish secure server-to-server type communications. Note: GSA PKI SSP device certificates are not publicly trusted and should not be used on public-facing websites or on websites with users outside the home agency.

Type	COMMON OID
Certificates to support secure HTTP connections with end users and servers providing interagency trust	id-fpki-common-devices or id-fpki-common-deviceHardware

Digital Signature Certificates

A digital signature certificate is used to digitally sign documents such as PDFs or Microsoft Word or digitally sign emails. An agency may also request a Digital Autopen signature certificate to sign documents for the *Federal Register*.

Type	COMMON OID
Certificates to digitally sign emails and documents	id-fpki-common-hardware

Key Management Services

Key Management Services store and manage private keys associated with encryption certificates. Examples might include Key Escrow and Recovery, Key History, and Data Decryption Services.

Conclusion

GSA established the GSA PKI SSP Program to help agencies identify and procure federally-compliant PKI services and digital certificates. There may be multiple types of PKI SSPsrs, but only one type of GSA PKI SSP. This clear definition not only helps agencies identify approved services, but also leverage the governmentwide acquisition vehicles for customer agencies to receive consistent pricing, terms, and services. The GSA PKI SSP Program Office maintains the SSP Program and coordinates government activity on behalf of the GSA PKI SSPs.

Appendix A - Sample MOA

Memorandum of Agreement
Federal Public Key Infrastructure
Shared Service Provider Program
(Commercial Entities Only)

This Memorandum of Agreement ("Agreement") is entered into by the General Services Administration, Office of Technology Policy (“OTP”), within the Office of Governmentwide Policy located at 1800 F Street, NW Washington, DC 20405 and the [name of the commercial SSP vendor ("Entity") located at [SSP vendor address], as of the date of OTP’s signature to this Agreement with a term of three years. The OTP and Entity will collectively be referred to as "Party" or the "Parties."

1. **Definitions**.
   a. Federal Public Key Infrastructure ("FPKI" or " Federal PKI") is an implementation of a set of PKI policies, processes, and information technology systems that provide the U.S. Government with a common baseline to administer certificates and public-private key pairs. Federal PKI is one of several trust frameworks supporting federated trust of government devices and persons used by the U.S. Federal Government.

   b. Federal Public Key Infrastructure Policy Authority ("FPKIPA" or " Policy Authority") is the federal trust framework governance body for a set of PKI systems and associated certificates used for federated trust across and between federal agencies and with entities that are not a U.S. Federal Government agency for mission delivery purposes. The Policy Authority is a group of representatives from U.S. Federal Government agencies (including cabinet-level departments) established pursuant to a charter under the Federal CIO council. It manages the policies governing the FPKI trust framework and approves or denies entities for certification into the trust framework.

   c. Shared Service Provider (“SSP”)
   An Entity that adheres to the FPKI set of policies and processes, as well as GSA requirements to provide digital certificate services to federal agencies.

   d. Shared Service Program (“SSP Program”) is a GSA program that provides technical support for the FPKI. Specifically, it supports the

governmentwide implementation of HSPD-12 and the FICAM Initiative. It is recognized as robust secure PKI services that provide agencies with the capability to implement secure logical and physical access to federal resources through outsourced shared PKI services. By cross-certification, the shared PKI infrastructure is a part of the FPKI's information technology systems governed by the FPKI.
GSA has established a Special Item Number (SIN) 541519PKI that identifies these PKI services that contract holders offer governmentwide.

2. **Purpose.** The purpose of this Agreement is to agree on the terms and conditions on which the Entity will participate in the SSP Program. The Office of Technology Policy (OTP) manages the SSP Program with managing partners from the following GSA offices:

   a. Office of Chief Information Security Officer ("OCISO")
   b. Federal Acquisition Service, Office of Information Technology Category ("ITC")
   c. Office of Government-wide Policy, Office of Technology Policy (OTP)

   Specifically, the OCISO manages the security posture of the Entity's information technology systems and the ITC makes the Entity's shared PKI services available for purchase through a GSA contract vehicle. External to but in concert with GSA, the FPKIPA governs the certificate policies, requirements, and practices for the shared PKI services. This Agreement sets forth the respective responsibilities and obligations of the Parties.

3. **Authority.** The basis of this Agreement and the subsequent inclusion of the Entity into the SSP Program aligns with the *Federal Information Security Modernization Act of 2014 (FISMA),* GSA's *IT Security Procedural Guide: Managing Enterprise Cybersecurity Risk CIO-IT Security-06-30 GSA Security Policy, the Federal Acquisition Regulation, the* federal PKI certificate policies, and the Entity certificate policy or practices listed in the Entity's MOA with the FPKIPA. It also complements the *SSP Operations Handbook*.

4. **Roles and Responsibilities of the Parties.**

   a. **The OTP will do the following:**
      i. Serve as the GSA senior official to grant the Entity's information technology system authorization to operate.
      ii. Determine program direction based on Federal Government need.
      iii. Ensure through the OCISO and ITC proper performance and delivery of PKI shared services.

iv. Develop and manage operational processes to effectively deliver the shared PKI services.
v. Represent SSP and SSP Program interests in the FPKIPA.
vi. Report quarterly on security posture to the FPKIPA and customer agencies.
vii. Coordinate service improvement and feedback from customer agencies to SSP.
viii. Collaborate with GSA managing partners to operate and maintain effective, secure, and reliable PKI services.

b. **The OCISO will do the following:**
   i. Serve as the GSA senior official to recommend the Entity's information technology system for authorization to operate (ATO).
   ii. Monitor and report on the Entity's information technology system security posture.
   iii. Provide quarterly security reports to the Authorizing Official.
   iv. Collaborate with the OTP on security management concerns to operate and maintain an effective, secure, and reliable PKI shared service.

c. **The ITC will do the following:**
   i. Own and manage SIN 541519PKI for the SSP Program on the GSA Multiple Award Schedule (MAS).
   ii. Review the Entity's MAS Information Technology Package for a contract determination.
   iii. Collaborate with OTP and the ITC contract team to make the Entity's PKI shared service available to purchase.
   iv. Collaborate with the OTP on contract management concerns to deliver effective, secure, and reliable PKI shared service.
   v. Issue and revoke certificates to approved SSPs

d. **The Entity will do the following:**
   i. Comply with all laws, ordinances, and regulations (Federal, State, or Local) covering work in the SSP Program.
   ii. Comply with the FPKI policies to the include the *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework (FCPF)*, hereafter referenced as COMMON and its complementary documents:
      1. Change proposals
      2. Key Recovery Policy
      3. U.S. Federal Certificate Profiles: X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Providers (SSP) Program

        4. Memorandum of Agreements (MOAs) established between the FPKIPA and Entity.

    iii. Obtain an Authorization to Operate (ATO) declaration through GSA's formal program for information security management before rendering PKI services.
    iv. Ensure adequate resources to maintain an ATO and comply with binding operational directives, and GSA requirements for protecting GSA IT resources. This includes addressing critical gaps (e.g., multifactor authentication, database encryption, no outdated software, high and critical findings, etc.) in the timeframe specified in GSA guidance.
    v. Ensure any certificates, associated certificates, and public key pairs issued to the federal agencies will be owned by the government.
    vi. Use the *SSP Operations Handbook* as the program's established guidelines while complying with regulations and GSA expectations.
    vii. Prepare for and facilitate monthly Security Dashboard and Plan of Action and Milestones meetings.
    viii. Attend and/or participate in monthly program, security, and contract meetings to exchange information or provide feedback on proposed changes to the program.

5. **Third Parties.** This Agreement is binding only upon the Parties, by and through their officials, agents, employees, and successors. Entity may not assign its rights or delegate its duties or obligations under this Agreement without prior written consent from OTP. No person or entity is intended to be a third-party beneficiary of the provisions of this Agreement for purposes of any civil, criminal, or administrative action, and accordingly, no third person or entity may assert any claim or right as a beneficiary or protected class under this Agreement in any civil, criminal, or administrative action.

   This Agreement does not authorize, nor shall it be construed to authorize, or add to any systems, documents or other technology, persons or entities not a Party to this Agreement nor intended to have authorization under this Agreement.

6. **Entity Change.** If Entity anticipates changes or has changed due to a merger, acquisition, bankruptcy, or other means that modifies the Entity ownership or security boundary, then Entity shall:

   a. Provide written notification to OTP about the intent to change the business relationship in a timely manner not to disrupt any PKI services.

b. Provide a transition plan that includes all activities from transferring a PKI solution to resolution of impacts on end users and the delivery environment. The depth of a transition plan should be appropriate for the type of transition and the criticality of the PKI components going through transition. At minimum, the activities in the transition plan must be compliant with the COMMON and address the following:

   i. The coordination and scheduling of transferring system archives, system inventory and configuration data, certificate profiles, key recovery databases (if applicable), private keys, key shares, audit records, hardware security modules, certificate and certificate revocation list (CRL) databases, and all policy and security documents applicable to the operations of the PKI solution.

   ii. The estimated costs for terminating, transferring, selling, or disposing a PKI solution must be shared if direct or indirect expenses are transferred to the new approved SSP and/or the impacted customer agency.

   iii. The continued services for all certificates, certificate revocation, and status checking until the expiration of the longest-lived certificate or transference of the control for the DNS Names in URLs for these services.

   iv. The continued support to collect and review system audit logs for the PKI solution.

   v. The continued support required to obtain and provide annual PKI compliance audits until revocation of all issued certificates or the expiration of the longest-lived issue certificate.

7. **Compliance with Laws, Regulations and Policies.** Entity agrees to comply with all applicable policies listed in Appendix A.

   The following is applicable if Entity is not a U.S. Federal Government agency: Entity shall comply with applicable U.S. Federal laws and regulations including but not limited to trade compliance, economic and trade sanctions, and blocked, denied, and debarred persons lists. If the Entity is not in compliance with these applicable laws and regulations, OTP reserves the right to change or remove the Entity's participation in the SSP Program in the interest of national security.

8. **Updates:** The OCISO and OTP are responsible for the maintenance and update of the *IT Security Procedural Guide: Managing Enterprise Cybersecurity Risk*

CIO-IT Security-06-30 GSA Security Policy and *SSP Operations Handbook* respectively.

Entity shall review the document updates each time they are updated and implement the necessary changes to practices to comply.

9. **MOA Updates and Evolving Security Requirements.** This MOA may be updated only by mutual written agreement signed by an authorized representative of each party.

   Notwithstanding the foregoing, due to the nature of evolving national security threats and updates to technology and security, the Parties shall work in good faith to implement required updates to applicable laws, regulations, and policies through the following steps:

   a. OTP, OCISO, or ITC will provide the Entity with written notice of the required updates, the number of days in which the updates must be implemented, and an updated version of Attachment A that incorporates the changes. The updated version of Attachment A will automatically replace the previous version of Attachment A and be deemed incorporated into this Agreement without further actions.

   b. Upon notification, the Entity shall have three (3) business days to confirm via written response whether it will be implementing the changes.

   c. If the Entity declines to implement the requirements, the OTP, ITC, and OCISO may decide to terminate this agreement, revoke ATO status, notify customer agencies of the situation, or take any such other action necessary to maintain the delivery of secure PKI services.

10. **Confidentiality.** If Entity is not a U.S. Federal Government agency, the following applies:

    a. Entity assumes full responsibility for and guarantees the security and confidentiality of all documents, data, and other information supplied or gleaned from the customer agency, Federal PKI, and provided, obtained, or accessed through being a party to this Agreement ("Confidential Information").

    b. Entity will prevent disclosure of this Confidential Information to any person not authorized by the U.S. Federal Government or Policy Authority to have access to such documents or information.

11. **Liability.** Neither Party shall be liable to the other for any loss, liability, damage or expense (including attorney fees) arising out of the operation of the PKI services. This Agreement is entered into for the convenience of the Parties and shall not give rise to any cause of action by Entity or by any third party.

12. **Conflict Resolution.** If Entity is a private sector entity, the Contract Disputes Act, 41 U.S.C. 7101 et seq, is applicable to all disputes under this Agreement.

13. **Governing Law.** This Agreement is governed by the laws of the United States.

14. **Termination.** If Entity is not in compliance with this Agreement or applicable security or technical requirements, the OTP shall notify the Entity and may unilaterally suspend participation in the SSP Program. The OTP shall provide the Entity an opportunity to cure the issues and regain its participation if there is a government business need as determined at the sole discretion of OTP. If the Entity does not cure within six months, OTP may terminate this Agreement in entirety. Either party may terminate this Agreement for convenience at its sole discretion with 30 days prior written notice.

    The Entity must provide a transition plan as described in Section 6 if termination is decided.

    This MOA is valid for one year from the last date in the signature section.

15. **System Disruption.** If there is a material issue in the operability of the PKI service in accordance with the documents in Section 3 that will have a substantial adverse effect on a customer's operations, OTP, the customer agency, OCISO, and Entity will determine a planned resolution within 10 days.

    Entity will promptly notify the OTP:

    a. In the event of any material problem or inability to operate Entity's certification authorities in accordance with the documents in Section 3.

    b. If the Entity becomes aware of a material noncompliance on the part of any other party that the Entity has formed an agreement with to use Entity's certification authorities covered by this agreement.

    c. If the Entity becomes aware of a material noncompliance on the part of supporting vendors that the Entity has formed an agreement covered by this agreement.

If the issue is a security incident, the Entity must comply with GSA's

Incident-Response-[CIO-IT-Security-01-02-Rev-19] and report incident to the OTP and OCISO, as well as submit an incident report for follow-on reporting to the Cybersecurity Infrastructure Security Agency (CISA), the Office of Inspector General (OIG), and the United States Congress, as applicable.

16. **Signatures:**

Name: Laura Stanton
Title: Assistant Commissioner
Organization: Federal Acquisition Service
Office: Office of Information Technology Category (ITC)

____

Name: Dan Pomeroy
Title: Deputy Associate Administrator
Organization: Office of Governmentwide Policy
Office: Office of Technology Policy (OTP)

____

Name: Bo Berlas
Title: Chief Information Security Officer
Office: Office of Chief Information Security (OCISO)

____