Memorandum of Agreement
Federal Public Key Infrastructure

This Memorandum of Agreement ("Agreement") is entered into by the United States Federal Public Key Infrastructure Policy Authority ("Policy Authority") located at 1800 F Street, NW Washington, DC 20405 and the United States Patent and Trademark Office (USPTO) ("Entity") located at 600 Dulany Street, Alexandria, VA 22314 as of the date of the Policy Authority's signature to this Agreement with a term of three years. Policy Authority and Entity will collectively be referred to as "Party" or the "Parties."

1. Definitions.

a. Public Key Infrastructure ("PKI") is a set of policies, processes, and information technology systems used for the purpose of creating, maintaining and revoking certificates and public-private key pairs. A PKI certificate is considered trusted based on the security requirements of the systems, the adherence to the agreed upon set of issuance procedures for asserting a claimed set of identity attributes in the public certificate, and protection of the associated private key. The certificate policy or Object Identifier ("OID") asserted in the public certificate is a public assertion of adherence to the requirements defined in a Certificate Policy ("CP") and implementation practices stated in a Certification Practice Statement ("CPS").

b. Federal Public Key Infrastructure ("FPKI" or "Federal PKI") is an implementation of a set of PKI policies, processes and information technology systems that provides the US 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 US Federal Government.

c. 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 US Federal Government agency for mission delivery purposes. The Policy Authority is a group of representatives from US 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.

d. Federal Public Key Infrastructure Management Authority ("FPKIMA" or "Management Authority") is governed under the FPKIPA. The FPKIMA operates and manages the certification authorities ("CA") that comprise the FPKI root certification authorities and/or bridge certification authority for the participating Federal agencies.

e. Entity is the organization operating a certification authority or non-federal trust framework certified by the Federal PKI Policy Authority. The certification is facilitated through the execution of this Agreement. The Entity is responsible for its adherence to the Agreement, as well as ensuring adherence to the Agreement by any external organization ("Entity Partner") public key infrastructure and / or certification authority system the Entity certifies.

f. Entity Customer is an organization that receives end entity certificates from one of the Entity operated certification authority systems certified by the Federal PKI Policy Authority.

g. Entity Partner is an organization external to the Entity that operates one or more certification authority systems that extends the Entity's trust relationship with the Federal PKI. Entity Partners inherit the requirements imposed by this Agreement through certification by the Entity.

2. **Purpose**. The purpose of this Agreement is to add Entity to the Federal PKI. The Policy Authority oversees and governs the certificate policies, requirements and practices for the public key infrastructure use cases in scope of Federal PKI. This Agreement sets forth the respective responsibilities and obligations of the Parties.

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

a. **Policy Authority will do the following:**

i. Publicly post the Certificate Policies.

Oversee the operations of the Federal PKI trust framework participants and systems in accordance with the Certificate Policies and Certification Practices Statements.

ii. Perform routine annual reviews of the Federal PKI trust framework participants, use cases, systems and related audits.

iii. Oversee and ensure, through the FPKIMA, proper performance of the operation and maintenance of the Federal PKI root certification authorities, and/or federal bridge certification authorities, in accordance with the Certificate Policies and Certification Practices Statements. This includes but is not limited to the following:

1. Private key protection.
2. Publish the CA and certificate status information publicly.

iv. Respond within a reasonable time to any requests for certificate policy, certificate practices and/or Annual Review Procedures information by the Entity.

v. Promptly advise the Entity of the following:

1. In the event of any material problem or inability to operate the Federal PKI root certification authorities, and/or federal bridge certification authorities in accordance with the Certificate Policies and Certification Practices Statements, or
2. In the event that the Policy Authority takes any action to terminate or limit other Federal PKI trust framework participants and systems.

b. **Entity will do the following:**

i. Provide the Policy Authority with access to necessary Entity information that includes but is not limited to compliance audit letters, operational information and testing processes in accordance with the Certificate Policies and the Annual Review Procedures.

ii. Operate and comply in accordance with the Certificate Policies and the Annual Review Procedures available at www.idmanagement.gov and meet the requirements in Attachment A.

iii. Respond within 10 days to requests for information by the Policy Authority or the FPKIMA.

iv. Make publicly available through the internet a repository containing the certificates, certificate status information and any other information necessary to support operation of Entity's certification authorities with all certification authorities that are in the Federal PKI trust framework.

v. Make publicly available an unredacted or redacted, depending on the applicable policies, version of Entity's Certificate Policy, Certification Practices Statement(s), and the annual PKI compliance audit Letter.

vi. In accordance with the annual review schedule, submit sample production subscriber certificates to the Policy Authority for all types of subscriber certificates issued by all of Entity's certificate authorities signed into or recognized as part of the Federal PKI trust framework.

vii. Attend and/or participate in Policy Authority working groups to provide feedback on proposed or enacted certificate policy and practices changes.

viii. Notify in writing the Policy Authority and Management Authority two weeks prior to creating or signing a new certification authority, changing certificate revocation list distribution points, changing online certificate status protocol universal resource indicators, and / or introduction new universal resource indicators or retiring universal resource indicators in the certificates.

4. **Third Parties**. Entity may not assign its rights or delegate its duties or obligations under this Agreement without prior written consent from the Policy Authority. 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.

5. **Entity Change**. If Entity anticipates changes or has changed due to a merger, acquisition, bankruptcy, or other means that adds additional entities to the Federal PKI, then Entity shall notify the Policy Authority in writing at least 30 days prior to making any such change.

   If the Entity is determined by the Policy Authority to be a national security risk due to these changes, then the Policy Authority may, in its sole discretion, temporarily suspend Entity's relationship with the Federal PKI, terminate this agreement or take other necessary actions.

6. **Compliance with Laws**. Entity agrees to comply with all applicable policies required for interoperability with the Federal PKI.

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

7. **Evolving Security Requirements**. Due to the nature of evolving national security threats and updates to technology and security, the Parties shall work in good faith to implement updated applicable laws, regulations, and policies. Attachment A includes security and technology requirements and will be reviewed and updated by the Policy Authority on a regular basis. This is to remove or update language due to changes in technology or security to ensure the requirements in this Agreement reflect current practices.

   The Parties agree that the Policy Authority may update this Agreement as it deems necessary by providing a written notice to Entity through the below process:

   a. The Policy Authority 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. Entity shall have 30 days to confirm via written notification to the Policy Authority whether it will be implementing the changes.

c. In the event that Entity declines to implement the changes, the Policy Authority may terminate this agreement, suspend or partially suspend Entity's authorization with the Federal PKI trust framework, or take any such other action necessary to maintain the operability and security of the Federal PKI.

Entity shall review the Federal PKI Certificate Policies each time they are updated and implement the necessary changes to policies and practices to be in compliance.

8. **Confidentiality.** If Entity is not a US 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 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 US Federal Government or Policy Authority to have access to such documents or information.

9. **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 Federal PKI. 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.

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

    b. If Entity is a US Federal Government Agency: Should disagreements arise on the interpretation of the provisions of this agreement or amendments and/or revisions thereto, that cannot be resolved at the operating level, the area(s) of disagreement shall be stated in writing by each party and presented to the other party for consideration. If agreement or interpretation is not reached within 30 days, the parties shall forward the written presentation of the disagreement to respective higher officials for appropriate resolution.

11. **Governing Law.** This Agreement is governed by US Federal law**.**

12. **Termination.** In the event that Entity is not in compliance with this Agreement or applicable security or technical requirements, the Policy Authority shall notify the Entity and may unilaterally change the policy mapping agreed upon or may revoke the Entity's participation in the trust framework. The Policy Authority 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 the Policy Authority. If Entity does not cure within six months, then the Policy Authority may terminate this Agreement in entirety.

    Either party may terminate this Agreement for convenience at its sole discretion with 30 days prior written notice.

13. **System Disruption.** In the event that there is a material issue in the operability of the Federal PKI in accordance with Federal PKI Certificate Policies that will have a substantial effect on the operations of the Federal PKI, the other Party will be notified within 10 days of the occurrence and the planned resolution.

    Entity will promptly notify the Policy Authority:
    a. In the event of any material problem or inability to operate Entity's certification authorities in accordance with the applicable Certificate Policy, Certification Practices Statements or supplemental requirements.

b. In the event that the Entity becomes aware of a material non-compliance 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. In the event that the Entity takes any action to terminate or limit such other party's interoperability with the Federal PKI.

d. Entity shall notify the FPKIMA and the Policy Authority in writing within 24 hours in the event of an Entity CA private key compromise or loss.

Federal PKI Policy Authority Co-chair:

MATTHEW ARNOLD Digitally signed by MATTHEW ARNOLD Date: 2021.01.19 14:33:36 -05'00'

Name: Matthew Arnold

Title: Acting Co-Chair, Federal PKI Policy Authority

Phone: (703) 254-6750

Email: matthew.arnold@gsa.gov

Date:

Entity Point of Contact:

Users, Mildrew, Sean Digitally signed by Users, Mildrew, Sean Date: 2021.01.12 16:35:55 -05'00'

Name: Sean Mildrew

Title: Deputy Chief Financial Officer

Phone: 571-270-7793

Email: Sean.Mildrew@USPTO.GOV

Date:

Federal PKI Policy Authority Co-Chair:

BALDRIDGE.TIM.W.1455368100 Digitally signed by BALDRIDGE.TIM.W.1455368100 Date: 2021.01.22 09:42:14 -06'00'

Name: Tim Baldridge

Title: Co-Chair, Federal PKI Policy Authority

Phone: (256) 288-0801

Email: tim.w.baldridge.civ@mail.mil

Date:

Entity Point of Contact:

Users, Holcombe, Henry Digitally signed by Users, Holcombe, Henry Date: 2021.01.14 08:28:03 -05'00'

Name: Henry J. Holcombe

Title: Chief Information Officer

Phone: 571-272-9400

Email: Jamie.Holcombe@USPTO.GOV

Date:

Attachment A
Technical and Security Requirements

1. **Maintain a Secure Environment**. Entity shall conduct, at a minimum, quarterly vulnerability scans and make patches/updates as necessary to maintain a secure environment.

2. **Identity Verification**. For certificate subjects, Entity shall ensure that the applicant's identity information is verified and confirmed in accordance with applicable certificate policies.

3. **Private Key Protection**. Entity shall protect the private key corresponding to the certificate authorities as required by the applicable certificate policies.

4. **Authorization to Operate**. If applicable, Entity shall maintain a current Federal Information Security Modernization Act Authorization to Operate (FISMA ATO) with the sponsoring agency, or with GSA. If GSA sponsors the FISMA ATO, the Entity shall abide by the current GSA IT Security Procedural Guide: Managing Enterprise Risk which is located at https://www.gsa.gov/about-us/organization/office-of-the-chief-information-officer/chief-information-security-officer-ciso/it-security-procedural-guides.

5. **Affiliated Organizations**.
    a. Entity shall ensure that subscriber certificates issued to an affiliated organization or agency customer accurately express the affiliation in compliance with Section 3 of the applicable Certificate Policies.
    b. Entity shall initiate and maintain agreements with affiliated organizations or agency customers that comply with the following:
        i. The affiliated organization or agency customer verifies the affiliation at the time of the certificate application.
        ii. The affiliated organization or agency customer requests revocation of the certificate when the affiliation ceases for any reason.

6. **Emergency Certificate Revocation Lists (CRLs).** If Entity or an Entity Partner becomes aware of a suspected or actual compromise of a private key used in the public-private key pair for a certificate, the Entity is responsible for ensuring an emergency revocation is performed and an updated certificate revocation list is published in accordance with the applicable certificate policies. The Entity shall notify the Policy Authority and Management Authority of the suspected or actual compromise of the private key(s) and the publication of the emergency certificate revocation list(s).

7. **Revocation of Certification Authority certificates**. An x509 certification authority certificate and / or an x509 cross-certificate may be revoked upon direction of the Policy Authority or upon a request by a designated official of the Entity. The Entity officials authorized to submit this revocation request are the signatories identified in this agreement and/or a delegated official of the Entity.

8. **Hardware Tokens**. If Entity or an Entity Customer is issuing PIV credentials containing certificates issued from the Entity's certification authorities, the Entity is responsible for ensuring the hardware tokens conform to the technical requirements referenced in the Federal Information Processing Standard Publication 201 and the hardware tokens are listed on a GSA approved products list.

9. **Certificate Policy and Certification Practice Statement(s).** The Entity certificate policies and practices associated with the Entity operated and / or Partner operated certification authorities referenced by this Memorandum of Agreement are:

Name of Document	Link to Publicly Posted Document
United States Patent and Trademark Office Public Key Infrastructure Certificate Policy (Version 2.9)	https://www.uspto.gov/sites/default/files/documents/uspto-pki-cert-policy.pdf
Certification Practices Statement for the United States Patent and Trademark Office (Version 3.1)	Not publicly posted

10. **Certificate Policy Mapping**. The certificate policies and practices associated with the Federal PKI Certificate Policies and the Entity Certificate Policies and / or Certification Practices Statements have been mapped according to the following table. The Federal PKI Policy authority may issue an x509 certificate and / or a letter of trust to one or more Entity or Entity partner operated certification authorities indicating this certificate policy mapping.

Federal PKI policy Object Identifier and Name	Entity policy Object Identifier and Name
2.16.840.1.101.3.2.1.3.2 id-fpki-certpcy-basicAssurance	2.16.840.1.101.3.2.1.2.7 pto-basic-2003
2.16.840.1.101.3.2.1.3.3 id-fpki-certpcy-mediumAssurance	2.16.840.1.101.3.2.1.2.8 pto-medium-2003
2.16.840.1.101.3.2.1.3.12 id-fpki-certpcy-mediumHardware	2.16.840.1.101.3.2.1.2.9 id-pto-mediumHardware
2.16.840.1.101.3.2.1.3.37 id-fpki-certpcy-mediumDevice	2.16.840.1.101.3.2.1.2.11 id-pto-mediumDevice
2.16.840.1.101.3.2.1.3.38 id-fpki-certpcy-mediumDeviceHardware	2.16.840.1.101.3.2.1.2.12 id-pto-mediumDeviceHardware