Submit the completed PIA to
Privacy’s SharePoint Customer Center

PIA for PKI

1. Contact Information

A/GIS Deputy Assistant Secretary
Bureau of Administration
Global Information Services

2. System Information

(a) Name of system: PUBLIC KEY INFRASTRUCTURE
(b) Bureau: IRM/FO/ITI/SI
(c) System acronym: PKI
(d) iMatrix Asset ID Number: 539
(e) Reason for performing PIA: Click here to enter text.
   - [ ] New system
   - [ ] Significant modification to an existing system
   - [x] To update existing PIA for a triennial security reauthorization
(f) Explanation of modification (if applicable): Click here to enter text.

3. General Information

(a) Does the system have a completed and submitted Security Categorization Form (SCF)?
   - [x] Yes
   - [ ] No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

(b) What is the security Assessment and Authorization (A&A) status of the system?
   Expired on 06/2016 and reassessment is in progress.

(c) Describe the purpose of the system:
   Public Key Infrastructure (PKI) is the framework and services that provide for the generation, production, distribution, control, and accounting of Public Key certificates. PKI is a potent tool that enhances computer security for the Department and gives users more options at the desktop such as encryption and digital signatures of e-mail. It enables e-commerce, secure web transactions, and provides privacy to users. PKI provides four basic features on the Department's SBU network: Privacy of Communication, Strong Authentication of Users, Integrity of Communications, and Non-Repudiation.

(d) Describe the personally identifiable information (PII) that the system collects, uses, maintains, or disseminates:
PKI does not contain PII within the system. DOS users submit the “Application for Token Request/Receipt Form” to the PKI Program Office in order to receive digital certificates. The form captures data to meet the minimum requirements for the Department’s high-assurance PKI. The information found in the Department’s Global Address List (GAL), such as the applicants’ name, office, telephone number, and email address is used. In addition, an individual’s identity from the identification numbers assigned to an individual’s documentation (e.g., post access badge, DOS I.D badge) is used. Authorized PKI Program Office staff verify an individual’s identity by using the identification numbers assigned to an individual’s documentation (e.g., post access badge, DOS I.D badge). This form is a paper form that must be completed and signed by the individual. With the exception of the information that identifies the identification of an individual, all information is provided by the applicant. The form is either stored electronically (via PKI Registration Center (PRC) mailbox or SI SHARE drive) or physically at SA-7B (permanent storage location), HST IT Mart (temporary storage location) and HST Rosslyn (temporary storage location). The forms are accessible only to the PKI Program Office.

Adoption Tracking Services (ATS) is an international adoption program that works with the Department, and relies on PKI certificates to provide user validation. ATS is owned by Consular Affairs/Overseas Citizens Services (CA/OCS) and is not logically connected to the Department’s PKI. For the users involved with ATS, name, organization, organization address, telephone and fax numbers, and email address are captured. The information is provided by the applicant when he or she applies for a certificate. Applicant’s name and email address are used in the certificates and are required. The other information is part of validating their identity. All non-Department employees on whom this data is collected, approximately 1.5% of the system users, are employees of approved partner organizations and agencies involved in the ATS program, which is supported by the Department of State to facilitate international adoptions. The information is collected with an electronic form titled Token Eligibility/Access Certification and Acknowledgement Form. The form sends the data via email to specified personnel within the PKI Program Office who will then review the data and publish it to the internal PKI and CA\ATS databases. In addition to the form information being emailed to PKI Program Office Personnel, all data is stored on an ESOC DMZ webserver allocated to PKI Program Office. Access to the data is managed by an access control list (ACL). The ESOC DMZ webserver where the data is stored is not encrypted as only name and email address (publicly disclosed information) are stored. The link to the form is below.

http://crls.pki.state.gov/ats/registration
(e) What are the specific legal authorities and/or agreements that allow the information to be collected?

The Department of State Public Key Infrastructure X.509 Certificate Policy (CP). The Department’s CP is derived from the Federal Bridge Certificate Policy. (In cryptography, X.509 is an ITU-T standard for a Public Key Infrastructure (PKI) and Privilege Management Infrastructure (PMI). X.509 specifies, amongst other things, standard formats for public key certificates, certificate revocation lists, attribute certificates, and a certification path validation algorithm.)

This CP was established under the authority of and with the approval of the Federal CIO Council. Under 44 U.S.C. § 3603, the CIO Council is authorized to develop and improve agency practices for the use and operation of Federal Government information resources. The Federal Information Security and Modernization Act, P.L. 113-283, requires agencies to comply with such policies, procedures, standards, and guidelines. 44 U.S.C. § 3554(a)(1)(B).

The Department implements the CP through a Memorandum of Agreement between the Federal PKI Policy Authority and the Department of State dated February 21, 2018.

(f) Is the information searchable by a personal identifier (e.g., name or Social Security number)?

☒ Yes, provide:
- SORN Name and Number: Network User Account Records STATE-56
- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN): December 12, 2017

☐ No, explain how the information is retrieved without a personal identifier. Click here to enter text.

(g) Does the existing SORN need to be amended to reflect the inclusion of this new or significantly modified system? ☐ Yes ☒ No

If yes, please notify the Privacy Division at Privacy@state.gov.

(h) Is there a records retention schedule submitted to or approved by the National Archives and Records Administration (NARA) for this system? ☒ Yes ☐ No

(If uncertain about this question, please contact the Department’s Records Officer at records@state.gov.)

Yes

If yes provide:
- Schedule number (e.g., (XX-587-XX-XXX)): N1-GRS-07-3 item 13a1 (GRS 3.2, item 60), item 13a2 (GRS 3.2, item 061), item13b (GRS 3.2, item 062).
- Length of time the information is retained in the system: Documentation within the PKI is retained for 20 years 6 months prior to transfer to the National Archives and Records Administration (NARA). This is a requirement from the Federal Bridge Certification Authority, and is not optional.
- Type of information retained in the system:
**Certificate and Certificate Revocation items**

### 4. Characterization of the Information

(a) What entities below are the original sources of the information in the system? Please check all that apply.
- ☒ Members of the Public Members of the public provide identical information as employees of the Department of State.
- ☒ U.S. Government employees/Contractor employees
- ☐ Other (people who are not U.S. Citizens or LPRs)

(b) If the system contains Social Security Numbers (SSNs), is the collection necessary?
- ☐ Yes  ☒ No (SSNs are not collected)

- If yes, under what authorization?
  Click here to enter text.

(c) How is the information collected?
The information is collected from Department employees via the Application for Token Request/Receipt Form. The information is collected from ATS participants via the Token Eligibility/Access Certification and Acknowledgement Form.

(d) Where is the information housed?
- ☒ Department-owned equipment
- ☐ FEDRAMP-certified cloud
- ☐ Other Federal agency equipment or cloud
- ☐ Other

- If you did not select “Department-owned equipment,” please specify.
  Click here to enter text.

(e) What process is used to determine if the information is accurate?
It is provided by the individuals when they request a certificate, and it is up to them to ensure the information they provide is accurate. The information provided by the applicants will be validated at the time of submission by checking against the information in the GAL. Should their name or email address be inaccurate, a new certificate would be issued upon request by the applicant.

(f) Is the information current? If so, what steps or procedures are taken to ensure it remains current?
The information is validated at the time of issuance of the smart card. The PKI team does not monitor for modifications after issuance. Whenever the user receives a new smart card, the user’s information is validated (at that time) and the smart card is issued.

(g) Does the system use information from commercial sources? Is the information publicly available?
No.

(h) Is notice provided to the individual prior to the collection of his or her information?
Yes, via Privacy Act Statements on the forms which collect the information needed for this system and the System of Records Notice, State-56.

(i) Do individuals have the opportunity to decline to provide the information or to consent to particular uses of the information? ☒ Yes   ☐ No

- If yes, how do individuals grant consent?
  Individuals may decline to provide the requested information. However, that would result in certificates not being issued.

- If no, why are individuals not allowed to provide consent?
  Click here to enter text.

(j) How did privacy concerns influence the determination of what information would be collected by the system?
Only authorized personnel can access the PKI system. They can access the lists of all personnel with certificates to manage that function. All administrative users of the PKI can view information on the users’ certificates, i.e., name and email address. Controls are in place to limit access to the system by non-administrators, i.e., two-person access controls (access to the system requires two trusted personnel) are in place to access the PKI facilities.

Only members of the PKI Program Office have access to the application forms containing the identifying data provided during application.

5. Use of information

(a) What is/are the intended use(s) for the information?

The information is only used to validate the identity of the users, and is part of the identifying data on the certificates. The data is not shared with any other organization or application.

(b) Is the use of the information relevant to the purpose for which the system was designed or for which it is being designed?

Yes, the information is only used to validate the identity of the users, and is part of the identifying data on the certificates.

(c) Does the system analyze the information stored in it? ☐ Yes   ☒ No

If yes:

(1) What types of methods are used to analyze the information?
  Click here to enter text.

(2) Does the analysis result in new information?
  Click here to enter text.

(3) Will the new information be placed in the individual’s record? ☐ Yes   ☐ No
6. Sharing of Information

(a) With whom will the information be shared internally and/or externally? Please identify the recipients of the information.

The information in the system is not shared with anyone internally or externally on a regular basis. However, there may be occasions when law enforcement or intelligence entities are given access with the appropriate approvals.

(b) What information will be shared?

All requested information available on the Application for Token Request/Receipt Form would be provided.

(c) What is the purpose for sharing the information?

The purpose of sharing information is for investigative purposes.

(d) The information to be shared is transmitted or disclosed by what methods?

Information would be provided in either hard-copy format, or emailed via encrypted mail.

(e) What safeguards are in place for each internal or external sharing arrangement?

Safeguards for sharing ensure that the identifying data included in the Application for Token Request/Receipt Form associated with the certificates can only be viewed by authorized recipients.

(f) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed?

Ensuring that PII is only made available on a need to know basis was a concern. That is why the approval process was put into place and the information is only shared with appropriate law enforcement or intelligence entities upon approval.

7. Redress and Notification

(a) What procedures allow individuals to gain access to their information?

Individuals would become aware of some part of their information being inaccurate by reviewing their certificate, reviewing the information within the GAL, and attempting to use the digital signing or encryption certificates issued to the card and receiving an error message when opening or sending emails with the aforementioned certificates. They would then contact the PKI Office to find out why they are receiving an error message thus potentially leading to having the information corrected.

(b) Are procedures in place to allow an individual to correct inaccurate or erroneous information?

☒ Yes ☐ No

If yes, explain the procedures.
Should the user identify that the name or email address in their certificate is inaccurate, or experience errors when trying to use their certificate, a new certificate would be issued upon request by the applicant.

If no, explain why not.

Click here to enter text.

(c) By what means are individuals notified of the procedures to correct their information?
After the request is received, an authorized individual will contact the requestor via email or phone.

8. Security Controls

(a) How is the information in the system secured?
Network identifying data, i.e., name and email address, is available in the certificates, and is visible to all users of the PKI, to include recipients of signed and encrypted email. Other data such as information concerning identifying documents is secured either in a secure physical location, or has been electronically scanned and sent to a secure location.

(b) Describe the procedures established to limit access to only those individuals who have an “official” need to access the information in their work capacity.
Only members of the PKI Program Office have access to the application forms containing the identifying data provided on the user applications.

(c) What monitoring, recording, and auditing safeguards are in place to prevent the misuse of the information?
Network identifying data, i.e., name and email address, is available in the certificates, and is visible to all users of the PKI, to include recipients of signed and encrypted email. Completed Application for Token Request/Receipt forms are scanned to a Shared drive with permissions set by Access Control List (ACL) that PKI Program Office staff assigned a PKI Trusted Role are authorized to access and secured at SA-7B in a storage cabinet within a secured room with a combination lock on the door. The combination is provided to staff designated as having a PKI Trusted Role which require access to the forms to perform their job functions. The PKI Program Office has a dedicated PKI Auditor who reviews the PKI system’s audit logs on a quarterly basis to ensure there are no anomalies.

(d) Explain the privacy training provided to authorize users of the system.
All users of the system are responsible for the issuance and management of PKI certificates. All are provided the PS800 Cyber Security Awareness course during their initial employment date and annually, which addresses the protection of government-owned information. All employees are required to take the mandatory FSI course, PA 459, Protecting Personally Identifiable information.

(e) Are any security controls, such as encryption, strong authentication procedures, or other controls, in place to make the information unusable to unauthorized users? ☒ Yes ☐ No
If yes, please explain.
The database in which the information is stored is encrypted. In addition, only authorized personnel can access the PKI system and manage, e.g., update and patch, the PKI application. Physical access to the system requires access to the facilities housing the systems, which can only be accessed under two-person control (as explained in 4(j)).

(f) How were the security measures above influenced by the type of information collected? The security measures were not influenced by the information collected. The FPKI is the governing body that provides policy and guidance for managing a federal PKI. The PKI is secured because of FPKI requirements.

9. Data Access

(a) Who has access to data in the system?
Only authorized personnel can access the PKI system. Only members of the PKI Program Office have access to the application forms containing the identifying data provided during application.

(b) How is access to data in the system determined?
Access to data in the system is determined by the roles and responsibilities for an individual in the IRM/FO/ITI/SI/IIB PKI Program Office. All users of the system are responsible for the issuance and management of the PKI system and the certificates it creates. All are provided the Cyber Security Awareness course, which addresses the protection of government-owned information.

(c) Are procedures, controls or responsibilities regarding access to data in the system documented? ☒ Yes   ☐ No

(d) Will all users have access to all data in the system, or will user access be restricted? Please explain.
Users do not have access to the system. Only authorized staff of the PKI Program Office have access to data in the system. Moreover, the certificate application forms containing the identifying data provided during certificate request are restricted to authorized staff of the PKI Program Office.

(e) What controls are in place to prevent the misuse (e.g. unauthorized browsing) of data by users having access to the data?
There are physical controls in place to prevent the misuse of data by users having access to the data. Two-person access control is in place to access this data and as well as the requirement to have authorized approval to physically access the ESOC datacenter facilities which the PKI Systems reside in. In addition, there are entrance/exit logs to document when access to the facilities housing the PKI system occurs and they are reviewed by the PKI auditor. All users having access to the system as PKI Trusted Roles have been vetted thoroughly by the U.S. Office of Personnel Management (OPM) presenting them with a Top Secret (TS) clearance or an interim TS. Users assigned a PKI Trusted Role are required by Federal Public Key Infrastructure (FPKI) policy to access system data in accordance to their day to day job responsibilities.