DEPARTMENT OF TREASURY
Washington, D.C. 20220

Treasury Public Key Infrastructure
Privacy Impact Assessment (PIA)

April 29, 2008

A. Identification

System Name: Public Key Infrastructure (PKI)
OMB Unique Identifier: 015-00-02-00-01-1070-00-404-140
System Owner: Office of the Chief Information Officer
Associate CIO E-Government

Contact — Director, Disclosure Services: Hugh Gilmore
Privacy Act Officer: Dale Underwood

Address: FOIA/PA Request
Disclosure Services
Department of the Treasury
Washington, D.C. 20220

Telephone: (202) 622-0930
Fax: (202) 622-3895

B. System Application/General Information:

1. Does this system contain any information in identifiable form?
Yes

2. What is the purpose of the system/application?

Treasury's PKI is a combination of policies, procedures and technology that provide a high degree of trust in Treasury personnel, systems and data. This degree of trust is achieved through the use of Treasury-issued digital certificates, objects created by highly secure systems known as Certification Authorities (CAs). Treasury certificates bind digital information to physical identities to allow a high degree of assurance to be placed in them.

The TOCA/TECA/TRCA systems represent a collection of hardware, software, and trusted roles. These CA's are capable of issuing certificates for several levels of assurance as defined in the Treasury X.509 Certificate Policy (CP) and their respective Certification Practices Statements (CPS). The TRCA serves as the "trust anchor" within the infrastructure, and as such, signs and issues cross-certificates between other Root CA's, and manages certificates for CA's within its trust domain, such as the TOCA and TECA. This system is also

implemented as a lights out operation, though it is offline (i.e. not connected to a computer network). The TOCA and TECA systems authenticate and register subscribers, create certificates, sign certificates, transmit certificates to a public directory, revoke certificates, and manage subscriber keys and certifi8cates. Managing certificates includes making revocation information available to subscribers. The TOCA and TECA systems are implemented as a lights-out operation available online at all times.

On November 18, 2004, the Treasury CIO Council approved transitioning the hosting, operations and maintenance of Treasury's Public Key Infrastructure (PKI) Certification Authorities to the Bureau of the Public Debt, as recommended by the PKI Executive Steering Committee. The CIO Council further identified Treasury's PKI infrastructure as the preferred source of PKI services for the Bureaus and Departmental Offices.

3. What legal authority authorizes the purchase or development of this system/application?

The Treasury PKI systems are included in the Capital Planning and Investment and Control (CPIC) process at the Department of the Treasury. The Clinger-Cohen Act of 1996 (CCA)[1] requires agencies to use a disciplined CPIC process to acquire, use, maintain, and dispose of information technology. The purpose of the CCA is to improve the productivity, efficiency, and effectiveness of federal programs though improved acquisition, use, and disposal of IT resources. The Department of the Treasury has implemented its IT governance processes to support CPIC which involve the selection and approval of programs and systems through the Office of Management and Budget (OMB). Therefore, the legal authority to purchase, development, and maintain the PKI systems is authorized annually through Treasury CPIC process. The Department of the Treasury posts its Exhibit 300 information to www.treas.gov. The PKI systems are contained within the Treasury investment titled "Enterprise IT Infrastructure Optimization Initiative (EITIO)"[2].

4. Under which Privacy Act SORN does the system operate?

Treasury .012 Fiscal Service Public Key Infrastructure (PKI) System

C. Data in the System:

1. What categories of individuals are covered in the system?

Federal employees, Government Contractors and Private Sector employees

2. What are the sources of the information in the system?

a. Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other source?

[1] http://www.cio.gov/Documents/it_management_reform_act_Feb_1996.html)
[2] http://www.treas.gov/exhibit300/2008/Enterprise-IT-Infrastructure-Optimization-Initiative%20_EITIO.pdf

Data is provided by the individual during the identity proofing process. Online directories also provide sources of data collected electronically.

b. What Federal agencies are providing data for use in the system?

Department of the Treasury, National Aeronautics and Space Administration and Department of Homeland Security

c. What State and/or local agencies are providing data for use in the system?

None

d. From what other third party sources will data be collected?
None

e. What information will be collected from the employee and the public?

Name, email and organization identifier

3. Accuracy, Timeliness, and Reliability

a. How will data collected from sources other than bureau records be verified for accuracy?

Certificate issuance practices require proofing of all submitted data. The data is also verified during an annual audit.

b. How will data be checked for completeness?

Certificate issuance requires a prescribed set of mandatory data elements. Therefore, all collected data is, by definition, complete.

c. Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date?

Yes. The certificate lifetime (3 years) is set by policy and can only be changed by authorized personnel as enforced by Treasury policies and system access controls. There is also language in the CPS requiring revocation in specific circumstances. Circumstances for revocation will include, but not be limited to instances where:

- Identifying information in the certificate become invalid;
- A Subscriber can be shown to have violated, or is suspected of violating, the certificate handling obligations as stipulated in the Subscriber Acknowledgement Form;
- Subscriber is no longer affiliated with Treasury;

- Subscriber Distinguished Name becomes invalid;
- A private key has been or is suspected of having been compromised, lost, or stolen;
- A Subscriber asks for his/her certificate to be revoked.

d. Are the data elements described in detail and documented?

Yes. Personal information retained by the system is defined by certificate issuance practices.

D. Attributes of the Data:

1. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

Yes

2. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?

The information that is collected is already available and verifiable by the authoritative systems. The system does not derive any new data.

3. Will the new data be placed in the individual's record?

Not applicable

4. Can the system make determinations about employees/public that would not be possible without the new data?

Not applicable

5. How will the new data be verified for relevance and accuracy?

Not applicable

6. If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?

Not applicable

7. If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access?

Not applicable

8. How will the data be retrieved?

Not applicable

9. What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?

Not applicable

E. Maintenance and Administrative Controls:

1. If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?

The system is operated from a single site. Public Debt will leverage its Contingency and Alternate Processing site to provide highly available Treasury Certificate Authority Operations.

2. What are the retention periods of data in this system?

Archives consist of the weekly backup copies of all PKI events and components as defined in the Treasury CP. Archives for TOCA and TECA are retained for 10 years, 6 months, while TRCA data is retained for 20 years, 6 months

3. What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?

Audit logs and Backups will be retained onsite for two weeks and then forwarded to an offsite secure storage facility (Iron Mountain) where they will be retained for a period of 10 years and 6 months from the date of creation. In the case of TRCA data, this is retained for 20 years and 6 months, per Treasury CP.

4. Is the system using technologies in ways that the bureau/office has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?

Yes

5. How does the use of this technology affect public/employee privacy?

The system publishes identity certificates to a publicly accessible repository. The identity information contained within these certificates is restricted to name, email address and organizational affiliation and may be obtained by other methods external to the system as well.

6. Will this system provide the capability to identify, locate, and monitor individuals?

No

7. What kinds of information are collected as a function of the monitoring of individuals?

Not applicable

8. What controls will be used to prevent unauthorized monitoring?

Public Debt's Rules of Behaviors prohibit the misuse of personal data stored in information systems.

9. Under which Privacy Act SORN does the system operate?

Treasury.012 Fiscal Service Public Key Infrastructure (PKI) System

10. If the system is being modified, will the Privacy Act SORN require amendment or revision?

No

F. Access to Data:

1. Who will have access to the data in the system?

CA Operator	• Backup of software, certificate database, and private keys to permit rebuilding in event of failure. • Serve as one of two parties controlling the signing certificate.
ISSO	• Ensure compliance with security policies in place. • Perform account and privilege management on CA equipment & workstations • Archive system records. • Perform weekly audit log review.
System Operator	• Perform operation and maintenance of CA hardware and operating system. • Install and maintain software. • Ensures continuous network connectivity. • Performs and stores backups.
Administrators	• Manage credentials • Issues credentials to subscribers
Auditor	• Ensure compliance with security policies and procedures

Subscribers	• Basic credential issuance and management, as restricted to the individual subscriber

2. How is access to the data by a user determined?

Access to data published to the directory by the system is anonymous (through directory queries) and need not be evaluated based upon a specific individual or role. Access to data stored on the system itself is restricted by the system's internal access controls, protected by multi-factor authentication procedures and further enforced through separation of duties.

3. Will users have access to all data on the system or will the user's access be restricted?

Access is restricted

4. What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access?

Public Debt network rules of behaviors prohibit the misuse of data contained in Federal information systems.

5. Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system?

Yes

6. Do other systems share data or have access to the data in the system?

Yes - Treasury Enterprise Directory Services (TEDS) and Treasury Self-Administration Server (TSAS)

7. Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?

Any interfaces would be required to be documented in an Interconnection Service Agreement. That document is a required part of the C&A package. Therefore, the Certification Officer and ISSO share this responsibility.

8. Will other agencies share data or have access to the data in this system (e.g. Federal, State, Local, and Others)?

No.

9. How will the data be used by the other agency?

Not applicable.

10. Who is responsible for assuring proper use of the data?

System owners whose applications are reliant on the PKI systems described here. Proper usage of these PKI systems from a policy perspective is the domain of the Department of the Treasury PKI Policy management Authority and is subject to audit.

###