ADAMS ML060580656

__X__ Yes __ No Make Public After President Submits Budget *(For OIS Use Only)*

U.S. Nuclear Regulatory Commission
Privacy Impact Assessment

Instructions: Section A, B, C, and D must be completed for all systems. Section E must be completed if yes is the answer to Section B, questions 1 and 2.

Date: February 17, 2006

A. GENERAL SYSTEM/APPLICATION INFORMATION

(See definitions at end of document)

1. Person completing this form:

Name	Title	Phone No.	Office
Mario Gareri	ICOD/NOSB/SSO	301-415-5527	T-4F34

2. System owner:

Name	Title	Phone No.	Office
Tom Rich	ICOD Division Director	301-415-7458	T-6F15

3. What is the name of this system?

Managed Public Key Infrastructure (MPKI)

4. Briefly describe the purpose of this system. What agency function does it support?

MPKI is a General Support System that is a federally compliant, partially outsourced service to provide digital certificates to NRC employees, contractors, and external partners. The digital certificates are used agency-wide by applications requiring strong user authentication, digital signature, and user-to-user encryption. MPKI includes processes for verifying the identity of certificate applicants, securely issuing certificates and keys, and revoking certificates in a timely manner. MPKI also escrows encryption keys of employees and contractors to prevent loss of data in the event a user's data encryption key becomes unavailable.

5. Note below whether this Privacy Impact Assessment supports a proposed new system or a proposed modification to an existing system.

_____New System __X__ Modify Existing System

B. PRIVACY ACT APPLICABILITY

1. Does this system collect, maintain, or disseminate personal information in identifiable form (e.g., name, social security number, date of birth, home address, etc.) about individuals?

   Yes __X*__ No ____

   *Employees, contractors, licensees, attorneys, vendors, general public, overseas foreign nationals. **Anyone** who has applied for or had a certificate amended, renewed, replaced, suspended, revoked, or denied.

2. If yes, will the data be retrieved by an individual's name or other personal identifier (e.g., social security number, badge number, etc.)?

   Yes __X__ No ___

If you answer yes to questions 1 and 2, complete Section E.

C. INFORMATION COLLECTION APPLICABILITY

1. Will the personal data be collected from or maintained by persons who are not Federal employees?

   Yes __X__ No _____

2. Will the data be collected from Federal contractors?

   Yes __X__ No ____

3. If the answer is yes to either question 1 or 2, will the data be collected from 10 or more persons during a calendar year?

   Yes __X__ No ____

4. If the answer is yes to question 3, is the information to be collected covered by an existing OMB clearance number? Yes ____ No __X__

   If yes, indicate the clearance number, 3150-

D. RECORDS RETENTION AND DISPOSAL SCHEDULE APPLICABILITY

Does this system already have a NARA-approved records disposition schedule? (Reference NUREG-0910, "NRC Comprehensive Records Disposition Schedule," or contact your office Records Liaison Officer or Jeff Bartlett, OIS.)

Yes _____ No __X__

If yes, list the records schedule number _____

Complete Section E only if the answers to Section B, questions 1 and 2 are Yes.

E. SYSTEM DATA INFORMATION

1. *Type* of information maintained in the system

a. Describe the information to be maintained in the system (e.g., financial, medical, training, personnel.) Give a detailed description of the data.

1. Subscriber Digital Certificates. These are X.509 standard certificates. The electronic certificate file includes the subscriber's name, e-mail address, organizational affiliation (e.g. NRC), and the cryptographic public key that corresponds to the private key in the subscriber's possession (e.g. on their workstation or smart card). Certificates are issued and labeled for different purposes, including digital signature, encryption, and authentication.

2. Public repository of digital certificates. To facilitate the use of digital certificates for data encryption and signature verification, the certificates are posted on a public web site hosted by Verisign, Inc., in accordance with the terms of OMB and GSA federal PKI commercial service provider policies. See OMB M-05-05.

3. Subscriber Encryption Certificate private keys. In order to minimize the likelihood of data loss in the event an NRC employee or contractor's encryption key becomes unavailable, the system places a copy of the key into a secure escrow, in accordance with the Federal PKI Common Policy (http://www.cio.gov/ficc/documents/CommonPolicy.pdf). Recovery of the cryptographic key requires a minimum of two authorized personnel with PKI Administrator certificates. Different portions of the data needed to recover the key are maintained at NRC and at Verisign.

4. MPKI audit data. In accordance with federal PKI policy (FBCA and Common Policy) audit data describing system transaction including certificate issuance, revocation, and key recovery, are maintained by the

system. When the audit data is aggregated, the name of the PKI Administrator performing the action is associated with the audit event. Different portions of the audit data are maintained at NRC and at Verisign.

5. Certificate revocation data. To facilitate the timely validation of certificates presented to an application, information about revoked certificates is maintained on publicly accessible web servers at Verisign. The Certificate Revocation List (CRL) is a digitally signed list of certificate numbers and revocation timestamps. The certificate number corresponds to the digital certificate posted on the public repository site.

6. Ordinary signature. Maintained in a filing cabinet in the Network Operations and Customer Service Branch of Office of Information Services for a period of a few months. Then the signature pages are scanned into ADAMS where they are retained for the remainder of the 10.5 years, non-publicly available, with limited access.

7. Subscriber Agreement. The Subscriber Agreement form is maintained in a filing cabinet in the Network Operations and Customer Service Branch for a period of a few months. Then the signed forms are scanned into ADAMS where they are retained for the remainder of the 10.5 years, non-publicly available, limited access. There will also be similar forms that are notarized coming to NRC from external subscribers. Those forms will also be stored in a filing cabinet within OIS/ICOD until they can be scanned into ADAMS.

2. *Source* of the data in this system

a. Are data being collected from the subject individual? If yes, what types of data are being collected?

Yes, name, e-mail address, organization, NRC badge number, ordinary signature, photograph, government-issued ID number (external subscriber).

b. Are data on this individual being collected from other NRC files and databases for this system? If yes, identify the files and databases.

No.

c. Are data on this individual being collected from a source or sources other than the subject individual and NRC records? If yes, what is the source and what type of data is being collected?

No.

d. How will data collected from sources other than the subject individual or NRC records be verified as current, accurate, and complete?

N/A

3. *Attributes* of the data

   a. Are the *data elements* described in detail and documented? If yes, what is the name of the document? Where is it located?

      Yes, the document is titled "Verisign NRC Engagement Summary," located in the MPKI Project Manager's working files.

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

      Yes.

   c. Will the system derive (i.e., create) new data or create previously unavailable data about an individual through aggregation from the information collected?

      Yes. The cryptographic key pair is new data bound to an individual. The public key is associated with the user's name and e-mail address in the public certificate.

      (1) How will aggregated data be maintained, filed, and utilized?

      The digital certificates, which consist of public keys, are maintained on a public web server at Verisign, and are used for verifying the validity of a private key. For example, if a document was signed electronically using a private key, the signature would be verified against the digital certificate located on the Verisign server. The digital certificates are filed by name and by email address.

      (2) How will aggregated data be validated for relevance and accuracy?

      The system compares the data with data on the NRC primary directory server (Novell eDirectory)

4. If data are consolidated, what *controls* protect it from unauthorized access, use, or modification?

   N/A

5. How will the data be *retrieved* from the system?

   a. Can it be retrieved by personal identifier? Yes __X__ No ___
   If yes, explain.

Certificates can be retrieved by name and by e-mail ddress from the VeriSign Digital ID Center.

b. Is a password or data description required? Yes _X__ No___
If yes, explain.

The VeriSign Digital ID Center requires no password as its purpose is to make certificates available to the public as widely as possible to facilitate secure communication. Separate components of the MPKI that are not linked to the Digital ID Center store more information related to the subscriber (date certificate was issued and by whom, if the certificate was revoked - date and by whom). These components are restricted to a small number of qualified MPKI Administrators and a special digital certificate is required for access.

6. Describe the report or reports that can be produced from this system.

a. What reports are produced from the system?

The Certificate Revocation List (CRL)

b. What are the reports used for?

Verifying that a certificate is still valid

c. Who has access to these reports?

The public

7. *Records retention*

a. What are the record types contained in this system and the medium on which they reside? (Examples: type - program records, medium - electronic; type - database, medium - electronic; type - system documentation, medium - paper.)

Type – application, medium – electronic; type – system documentation, medium – electronic.

b. What is the NARA-authorized retention period for each records series in this system?

The NARA retention schedule for PKI records is currently under development at NARA.

c. If unscheduled, what are your retention requirements for each records series in this system?

For PKI transaction and audit records, 10.5 years. For system administration records, 2 weeks. Certificates are currently valid for one year. This is expected to increase to 2 and possibly to 3 years in some cases.

d. What are the procedures for disposing of the data at the end of the retention period (specifically address paper copy, magnetic, or other forms of media)?

These will be as stated in MD 12.5 or its replacement as in effect in 2016.

e. How long will produced reports be maintained?

10.5 years.

f. Where are the reports stored?

At Verisign in Mountain View, California.

g. Where are the procedures for maintaining the data/reports documented?

In binder.zip, file location provided above.

h. How will unused or unwanted reports be disposed of?

Electronic file delete.

8. Capability to *monitor individuals*

a. Will this system provide the capability to identify, locate, and monitor (e.g., track, surveillance) individuals? ____Yes __X__ No. If yes, explain.

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

N/A

9. Coverage Under Existing *Privacy Act System of Records*

a. Under which Privacy Act System of Records (SOR) notice does this system operate (link to list of SOR available on NRC Internal Home Page)? Provide number and name.

No current system of records to cover MPKI.

b. If the Privacy Act System of Records is being modified, will the SOR notice require amendment or revision? ___ Yes ___ No.
If yes, explain.

10. *Access* to the Data

a. Who will have access to the data in the system (users, managers, system administrators, developers, other)?

Users, managers, system administrators, PKI administrators, the public.

b. Are criteria, procedures, controls, and responsibilities regarding access documented? If so, where?

Certificate Policy, (CP) Certification Practice Statement, (CPS) and procedures in binder.zip.

c. Will users have access to all data in the system or will users' access be restricted? Explain.

Users can access their own private keys, revoke their own certificates, and access the public repositories.

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

Private key recovery requires a minimum of two authorized administrators with admin certificates and key recovery privilege. Viewing audit data requires administrator privileges.

e. Do other systems share data or have access to data in this system?
Yes __X__ No ___ . If yes, explain.

The NRC primary eDirectory provides the user's name and email address for verification, and stores the user's NRC badge number and photograph for PKI audit purposes.

f. Will other agencies share data or have access to data in this system (Federal, State, local, other)? ___ Yes ___ No. If yes, explain.

Only to the public repositories.

g. Were Privacy Act clauses cited (or will be cited) and were other regulatory measures addressed in contracts with contractors having access to this system? _X__Yes ___ No. If yes, explain.

NARA PKI requirements, FBCA CP, and FPKI Common Policy CP.
http://archives.gov/records_management/policy_and_guidance/pki.html.

DEFINITIONS

Personal Information is information about an identifiable individual that may include but not be limited to:

- race, national or ethnic origin, religion, age, marital or family status
- education, medical, psychiatric, psychological, criminal, financial, or employment history
- any identification number, symbol, or other particular assigned to an individual
- name, address, telephone number, fingerprints, blood type, or DNA

Aggregation of data is the taking of various data elements and then turning them into a composite of all the data to form another type of data such as tables or data arrays, or collecting data into a single database.

Consolidation means combining data from more than one source into one system, application, or process. Existing controls for the individual parts should remain or be strengthened to ensure no inappropriate access by unauthorized individuals. However, since individual pieces of data lose their identity, existing controls may actually be diminished; e.g., a summary census report may not point at the individual respondent but rather at a class of respondents, which makes it less personal.

PRIVACY IMPACT ASSESSMENT REVIEW/APPROVAL
(For Use by OIS Staff)

System Name: **Managed Public Key Intrastructure (MPKI)**

Submitting Office: **Office of Information Services**

A. PRIVACY ACT APPLICABILITY REVIEW

____ Privacy Act is not applicable.

____ Privacy Act is applicable. Currently covered under System of Records, NRC _____. No modification to the system notice is required.

__X__ Privacy Act is applicable. Creates a new system of records. FOIA/PA Team will take the lead to prepare the system notice.

____ Privacy Act is applicable. Currently covered under System of Records, NRC _____. Modification to the system notice is required. FOIA/PA Team will take the lead to prepare the following changes:

Comments:

Through consultation with OGC, a decision was made that the MPKI should be officially noticed as a Privacy Act system of records, including all components and documentation collected and maintained in support of the life cycle of the digital certificates.

Although staff/contractors have stated that currently information is not routinely retrieved by an individual's name or personal identifier, it has been decided that since GSA has a published (official) Privacy Act system of records (GSA/GOVT 5, "Access Certificates for Electronic Services) it is in NRC's best interest to publish a system of records to ensure agency compliance knowing the type of data that is, or will be collected as the identity management roadmap expands, and to cover NRC for any anticipatory uses of the records.

The FOIA/PA Team/OIS will take the lead on preparing a system of records notice for publication in the Federal Register. They will contact the sponsoring office to explain the steps involved and to obtain the additional information needed.

Reviewer's Name	Title	Date
Sandra S. Northern	Privacy Program Officer	March 23, 2006

B. INFORMATION COLLECTION APPLICABILITY DETERMINATION

__X__ No OMB clearance is needed.

____ OMB clearance is needed.

____ Currently has OMB Clearance.

Comments:

MPKI is a General Support System that provides digital certificates to agency employees, contractors, and external partners and collects types of information such as name, e-mail address, organization, etc., used to identify the individual accessing the system. The information individuals provide is used to allow them access into the system, and it identifies them in a routine, non-intrusive, non-burdensome way. Inquiries which certify the identity of an individual in a non-intrusive way is not considered an information collection, so no OMB clearance is needed.

Reviewer's Name	Title	Date
Christopher J. Colburn	Team Leader	03/08/06

C. RECORDS RETENTION AND DISPOSAL SCHEDULE DETERMINATION

__X__ Additional information is needed to complete assessment.

__X__ Needs to be scheduled.

____ Existing records retention and disposition schedule covers the system - no modifications needed.

____ Records retention and disposition schedule must be modified to reflect the following:

Comments:

Issues regarding the material provided need to be clarified and appropriate schedule established. Issues identified include:

1) Item E.3.a indicates that documentation is maintained in a network shared drive, this is not a approved recordkeeping system.

2) Item E.7.b states that NARA is working on a schedule for PKI records, but we are not aware of this. NRC needs to establish a disposition schedule for our PKI records and submit it to NARA for review and approval.

3) Item E.7.c indicates that transaction records need to be maintained for 10.5 years. This is incorrect. They will need to be kept for the life of the record that the signature was attached to. For example, if the record submitted with a PKI is a 40 year record, the certification of the transaction will have to maintained for the same length of time.

4) Item E.7.d indicates that retention procedures will be included in MD 12.5 or its replacement in 2016. This is incorrect. According to the PMM, isn't this information required as part of the decommissioning plan that needs to be developed as part of the accreditation process?

These and additional records management issues will need to be resolved. However, the need for further records evaluation does not preclude moving forward with the system certification.

Reviewer's Name	Title	Date
Jeff Bartlett	Senior Records Analyst	3/16/06

D. BRANCH CHIEF REVIEW AND CONCURRENCE

____ Does not constitute a Privacy Impact Assessment required by the E-Government Act of 2002

__X__ Does constitute a Privacy Impact Assessment required by the E-Government Act of 2002 and requires approval of the Director, IRSD.

CONCUR IN REVIEW: **R/A** DATE: **03/23/2006**

Brenda J. Shelton, Chief
Records and FOIA/Privacy Services Branch

E. DIVISION DIRECTOR APPROVAL OF PRIVACY IMPACT ASSESSMENT:

(Approval is only required when Yes is given to Section B, questions 1 and 2 and Section C, question 1. The system collects, maintains, or disseminates personal information in identifiable form about members of the public.)

R/A DATE: **03/23/2006**

John J. Linehan, Director, Information and Records Services Division

TRANSMITTAL OF PRIVACY IMPACT ASSESSMENT/
PRIVACY IMPACT REVIEW RESULTS

TO: (Sponsoring Office) **Office of Information Services**	Office Sponsor**:** **Thomas Rich, Director, ICOD/OIS**	
Reginald Mitchell, Director Business Process Improvement and Applications Division, OIS	Name of System **Managed Public Key Infrastructure (MPKI)**	
Kathy L. Lyons-Burke, CISSP Senior IT Security Officer (SITSO)/ Chief Information Security Officer (CISO) Office of Information Services	Date Received: **02/22/2006**	Date Completed: **03/23/2006**

Noted Application Development and System Security Issues:

The MPKI should be officially noticed as a Privacy Act system of records, including all components and documentation collected and maintained in support of the life cycle of the digital certificates. The FOIA/PA Team will take the lead to prepare and publish the system notice. A copy of the published notice and effective date will be provided to the recipients listed above.

No information collection issues.

Additional records management information is required. However, the need for further records evaluation does not preclude moving forward with the system certification.

Brenda J. Shelton, Chief Records and FOIA/Privacy Services Branch, OIS	Signature: **R/A**	Date: **03/23/2006**