

U.S. Nuclear Regulatory Commission

Updated Privacy Impact Assessment

(Designed to collect the information necessary to make relevant determinations regarding the applicability of the Privacy Act, the Paperwork Reduction Act information collections requirements, and record management requirements.)

Authentication and Credentialing Services (ACS) System (formerly the Managed Public Key Infrastructure)

Updated: August 12, 2009

A. GENERAL SYSTEM INFORMATION

1. Provide brief description of the system:

Authentication and Credentialing Services (ACS), formerly known as Managed Public Key Infrastructure (MPKI), is a General Support System that is a federally compliant, partially outsourced public key infrastructure (PKI) service to provide digital certificates and other credentialing services to NRC employees, contractors, and external partners.

2. What agency function does it support?

The digital certificates are used agency-wide by applications requiring strong user authentication, digital signature, and user-to-user encryption. ACS includes processes for verifying the identity of certificate applicants, securely issuing certificates and keys, and revoking certificates in a timely manner. ACS also escrows encryption keys of employees and contractors to prevent loss of data in the event a user's data encryption key becomes unavailable.

3. Describe any modules or subsystems, where relevant, and their functions.

The system has five modules and the functions of these modules are described below.

Legacy Internal Staff (Software certificates only)

The Legacy Internal Staff subsystem supports the Broadband Remote Desktop (BRD) Citrix service provided by the NRC. Users present their agency identification (ID) badge and network ID in person at a help desk to receive a digital certificate. The Legacy Internal Staff ACS Application Server stores information about enrollments and certificates encrypted in the agency enterprise

directory system.

Internal Staff (All certificate types)

The Internal Staff subsystem implements [Federal Information Processing Standard \(FIPS\) 201](#), “Personal Identity Verification (PIV) of Federal Employees and Contractors” and the “X.509 Certificate Policy for The U.S. [Federal PKI Common Policy](#) Framework.” The Internal Staff subsystem uses services procured under the General Services Administration (GSA) Federal PKI Shared Service Provider program to issue digital certificates and smart card credentials to agency employees and contractors that are interoperable with other government agencies. For more information about the PKI Shared Service Provider program, see Office of Management and Budget (OMB) Memorandum M-05-05.

External Partner (All certificate types)

The External Partner subsystem uses services that are cross-certified with the Federal Bridge Certification Authority (FBCA) as PIV-Interoperable for use by non-Federal entities. This allows credentials issued by the NRC to its external partners to be recognized by other agencies and organizations. The External Partner subsystem issues digital certificates and smart card credentials at various e-authentication assurance levels to support the use of a range of NRC e-Government applications.

Certification Authority

The Certification Authority (CA) subsystem is outsourced infrastructure operated at vendor facilities under the terms and conditions of the GSA accredited Shared Service Provider program for shared use by multiple customers. The agency PKI Shared Service Provider is VeriSign, Incorporated, of Mountain View, California, (VeriSign). The CA creates digital certificates as requested, and hosts public directories of certificates and certificate revocation lists on behalf of the agency.

Authentication Service Bureau

The Authentication Service Bureau subsystem is an outsourced identity verification service operated by VeriSign. The Authentication Service Bureau receives enrollment and identification information from external partner applicants directly and through the External Partner subsystem. The information and documents are evaluated for accuracy and employment at NRC-affiliated organizations may be verified. The service is used to help meet federal requirements for identity proofing of applicants for higher assurance level credentials.

4. Points of Contact:

Project Manager	Office/Division/Branch	Telephone
Roger Swiger	OIS/ICOD	301-415-7553

Executive Sponsor	Office/Division/Branch	Telephone
Thomas Rich	OIS/ICOD	301-415-7458

5. Does this Privacy Impact Assessment (PIA) support a proposed new system or a proposed modification to an existing system?

a. New System Modify Existing System Other (Explain)

b. If modifying an existing system, has a PIA been prepared before?

Yes.

(1) If yes, provide the date approved and ADAMS accession number.

The MPKI PIA was approved 03/23/2006. ADAMS accession number is ML060580656.

B. INFORMATION COLLECTED AND MAINTAINED

(These questions are intended to define the scope of the information requested as well as the reasons for its collection. Section 1 should be completed only if information is being collected about individuals. Section 2 should be completed for information being collected that is not about individuals.)

1. INFORMATION ABOUT INDIVIDUALS

a. Does this system maintain information about individuals?

Yes.

(1) If yes, what group(s) of individuals (e.g., Federal employees, Federal contractors, licensees, general public) is the information about?

ACS maintains information about **anyone** who has applied for or had a certificate amended, renewed, replaced, suspended, revoked, or denied. The groups of individuals include Federal employees, Federal contractors, licensees, attorneys, vendors, general public, and overseas foreign nationals.

b. What information is being maintained in the system about individuals (describe in detail)?

(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, a certificate lookup service is hosted on a public web site at the Shared Service Provider facility.

(3) Subscriber Encryption Certificate private keys. This item applies to Internal Staff and Legacy Internal Staff subsystems only. 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. 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) PKI audit data. In accordance with federal PKI policy (FBCA and Common Policy) audit data describing system transactions including applicant enrollment, identity proofing, 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 the Shared Service Provider.

(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 the Shared Service Provider. The Certificate Revocation List (CRL) is a digitally signed list of certificate serial numbers and revocation timestamps. The certificate serial number corresponds to the digital certificate posted on the public repository site.

(6) Ordinary signature. Certain enrollment forms and subscriber agreements may require an ink signature.

(a) For the Legacy Internal Staff subsystem, these are maintained in a filing cabinet in the Network Operations and Customer Service Branch of the Office of Information Services (OIS) for a period of a few months. Then the signature pages are scanned into the Agencywide Documents Access and Management System (ADAMS) where they are retained for the remainder of the 10.5 year retention period, non-publicly available, with limited access.

(b) For the External Partner subsystem, signed documents are kept at the Authentication Service Bureau for a period of several months. Then they are shipped back to the Program Manager who then delivers them to the OIS records manager in the

Information and Records Services Division. They are retained for the remainder of the required retention period as determined by Federal Bridge assurance level requirements, non-publicly available, with limited access.

(7) Subscriber Agreement. The Subscriber Agreement may include identity proofing data such as name, home address, and date of birth. For the Legacy Internal Staff and Internal Staff subsystems, the Subscriber Agreement form is maintained as explained in item 6(a) above.

For the External Partner subsystem it is the same as paragraph 6(b) above.

(8) Driver's License Verification. For External Partner applicants at higher assurance levels, the applicant's driver's license number will be validated using a commercial service that accesses state motor vehicle department data to confirm that the license number, name, address, and date of birth are current and valid. The Authentication Service Bureau performs this step and records the result. No other information about the driver is requested or stored.

(9) Digital Fingerprint Images (Internal Staff PIV only). As required by FIPS 201, digital fingerprint images are taken of the applicant and stored encrypted in the Internal Staff subsystem. The fingerprint images are used to initiate the required federal background investigation process, and to confirm the identity of the applicant when picking up or replacing his or her PIV card.

c. Is the information being collected from the subject individuals?

Yes.

(1) If yes, what information is being collected from the individuals?

From internal staff: name, date of birth, organization, job function, e-mail address, telephone number, NRC badge number, ordinary signature, security clearance level, emergency responder role, photograph, fingerprints.

From external partners: name, date of birth, home address, home telephone number, organizational affiliation, business address, business telephone number, driver's license number or photocopy, other government-issued ID number or photocopy, ordinary signature.

d. Will the information be collected from 10 or more individuals who are **not** Federal employees?

Yes.

(1) If yes, does the information collection have OMB approval?

No, the collection of this type of information is considered exempt under the Paperwork Reduction Act of 1995.

(a) If yes, indicate the OMB approval number:

e. Is the information being collected from internal files, databases, or systems?

Yes, for internal staff only, information is collected to ensure accuracy and consistency of information used for PIV credentials.

(1) If yes, identify the files/databases/systems and the information being collected.

Integrated Personnel Security System (IPSS) provides staff member name, organization, and security clearance level.

f. Is the information being collected from an external source(s)?

No. Information provided by external partner applicants at higher assurance levels is verified against state and public records for accuracy.

(1) If yes, what are the sources and what type of information is being collected?

Not applicable.

g. How will this information be verified as current, accurate, and complete?

For internal staff, information is collected from the IPSS to ensure accuracy and consistency of information used for PIV credentials.

For External Partner applicants at higher assurance levels, the applicant's driver's license number will be validated using a commercial service that accesses state motor vehicle department data to confirm that the license number, name, address, and date of birth are current and valid. The Authentication Service Bureau performs this step and records the result. No other information about the driver is requested or stored.

In addition, external partner company names are verified against Secretary of State business records and company affiliation is verified through a telephonic employment check.

h. How will the information be collected (e.g. form, data transfer)?

Information from the IPSS is a data transfer. Otherwise, information is collected from online registration and paper forms completed by the applicant.

- i. What legal authority authorizes the collection of this information?

5 U.S.C. 301; Electronic Government Act of 2002, 44 U.S.C. Chapter 36; the Paperwork Reduction Act of 1995, 44 U.S.C. 3501; Government Paperwork Elimination Act, 44 U.S.C. 3504; Homeland Security Presidential Directive 12 (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004; Executive Order 9397.

- j. What is the purpose for collecting this information?

The purpose for collecting this information is for the verification of the identity of applicants for electronic credentials for access to federal facilities, internal computer systems, and Internet-based e-Government applications.

2. INFORMATION NOT ABOUT INDIVIDUALS

- a. What type of information will be maintained in this system (describe in detail)?

Not applicable.

- b. What is the source of this information? Will it come from internal agency sources and/or external sources? Explain in detail.

Not applicable.

- c. What is the purpose for collecting this information?

Not applicable.

C. USES OF SYSTEM AND INFORMATION

(These questions will identify the use of the information and the accuracy of the data being used.)

- 1. Describe all uses made of the information.

The information is used to verify the identity, organizational affiliation, identity credentials presented, and other attributes that may be asserted by an applicant for the issuance or renewal of an electronic identity credential. In the event of possible misrepresentation or misuse of an NRC-issued credential, the

information will be used to reconstruct identity proofing and registration events and may be turned over to law enforcement.

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

Yes.

3. Who will ensure the proper use of the information?

The system owner, assisted by the Information System Security Officer, will ensure the proper use of the information.

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

Yes.

- a. If yes, what is the name of the document that contains this information and where is it located?

The System Architecture Design Document which is located on the MPKI SharePoint site.

5. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?

No. The digital certificate and cryptographic key pair is new data bound to an individual.

- a. If yes, how will aggregated data be maintained, filed, and utilized?

Not applicable.

- b. How will aggregated data be validated for relevance and accuracy?

Not applicable.

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

Not Applicable.

6. How will the information be *retrieved* from the system (be specific)?

The public can retrieve certificates by name and by e-mail address from (<https://digitalid.verisign.com/services/client/index.html>) the VeriSign Digital ID Center. This service is available to anyone on the Internet.

Internal agency access to information in ACS will be by name. The Personnel Security Branch, Office of Administration (ADM), may retrieve information using name and/or Social Security Number.

7. Will this system provide the capability to identify, locate, and monitor (e.g., track, observe) individuals?

No.

- a. If yes, explain.

Not applicable.

- (1) What controls will be used to prevent unauthorized monitoring?
Not applicable.

8. Describe the report(s) that will be produced from this system.

The Certificate Revocation List (CRL)

- a. What are the reports used for?

The CRL is used to verify that a certificate is still valid.

- b. Who has access to these reports?

The public has access to this report.

D. RECORDS RETENTION AND DISPOSAL

(This question is intended to establish whether the information, data, or records contained in this system has an approved records retention schedule. (Reference NUREG-0910, NRC Comprehensive Records Disposition Schedule.)

1. Has a retention schedule (either under the General Records Schedule or NRC-specific) for this system been approved by the National Archives and Records Administration?

An NRC retention schedule for PKI has been written.

- a. If yes, list the schedule number and approved disposition.

N1431093

2. If you answered "No" to question D.1, complete the following section.

- a. Does the information in the system:

Have historical value?

Document NRC business decisions?

Contain data used to make a judgment or conclusion?

Provide statute or required regulatory information?

b. What is the value of the information to your organization and the Agency?

(1) When will it no longer be needed?

c. How will information, no longer required for current business operations, be maintained?

(1) Will it be separated from currently active information?

d. Does this electronic information system replace a previously "paper-based" information file system?

(1) If so, which files?

E. ACCESS TO DATA

1. INTERNAL ACCESS

a. What organizations (offices) will have access to the information in the system?

Currently the NRC offices with access to the information are the Office of Federal and State Materials and Environmental Management Programs (FSME), ADM, and OIS. Eventually this will include all NRC offices when a central identity repository is in place.

(1) For what purpose?

OIS accesses the information to manage the applicant enrollment and validation process leading to issuing a credential. Other offices will access the information to provide Program Sponsor approval of a credential application, and to verify an application user's credential status.

(2) Will access be limited?

Yes.

- b. Will other systems share or have access to information in the system?

When physical and logical access systems are implemented at the NRC as part of the federal HSPD-12 program, those systems may have access to information concerning internal staff credentials for validation only. NRC e-Government applications may have access to external partner credential information when a controlled access mechanism is available.

- c. How will information be transmitted or disclosed?

Non-public information is only disclosed to an approved Program Sponsor within the secure workflow when the Sponsor is notified of an application pending his or her review.

- d. What controls will prevent the misuse (e.g., unauthorized browsing) of information by those having access?

All privileged role holders within ACS must meet qualifications and sign special Rules of Behavior for Trusted Persons. Private Key recovery requires a minimum of two authorized administrators with administrator certificates and key recovery privilege. Viewing audit data requires administrator privileges.

- e. Are criteria, procedures, controls, and responsibilities regarding access documented?

Yes.

- (1) If yes, where?

In ADAMS at:
Trusted Access Requirements, ML081360011
Trusted Person Agreement, ML081080093
System Security Plan, ML080840567

2. **EXTERNAL ACCESS**

- a. Will external agencies/organizations/public share or have access to the information in this system?

Yes, but only to information about an individuals' **public** credentials which are located in the Public Certificate Repository portion of the ACS.

- (1) If yes, who.

All agencies, organizations, and the public.

- b. What information will be shared/disclosed and for what purpose?

The public certificates are accessible to foster secure communication, and the Certificate Revocation List to allow those relying on the certificates to check the revocation status.

- c. How will this information be disclosed?

Access to Certificates is by Web site using HTTPS and requiring search criteria to retrieve a certificate. Access to the digitally signed Certificate Revocation List is freely available by HTTP and LDAP.

F. TECHNICAL ACCESS AND SECURITY

1. Describe security controls used to limit access to the system (e.g., passwords). 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 ACS 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 ACS Administrators and a special digital certificate is required for access.

2. Will the system be accessed or operated at more than one location (site)?

Yes, at NRC offices and at Shared Service Provider facilities.

- a. If yes, how will consistent use be maintained at all sites?

All use and operation of the ACS system regardless of location is governed by the [VeriSign Shared Service Provider Certification Practices Statement](#) for internal staff services, and the [VeriSign Non-Federal Shared Service Provider PKI Certification Practice Statement](#) for external partner services.

3. Which user group(s) (e.g., system administrators, project manager, etc.) have access to the system?

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

4. Will a record of their access to the system be captured?

All access is audited and stored in logs of the respective subsystems and components.

- a. If yes, what will be collected?

User ID, full name, and time for all login events are collected. Audit information for security-related events also includes system activity performed.

5. Will contractors have access to the system?

Yes.

- a. If yes, for what purpose?

Contractors are part of the development and integration team for the system. They are also part of the operations and maintenance team. Contractors will also have user access to enter their information to obtain a credential.

- *Ensure that the following Federal Acquisition Regulation (FAR) clauses are referenced in all contracts/agreements/purchase order where a contractor has access to a Privacy Act system of records to ensure that the wording of the agency contracts/agreements/purchase order make the provisions of the Privacy Act binding on the contractor and his or her employees:*
 - 52.224-1 Privacy Act Notification.
 - 52.224-2 Privacy Act.

6. What auditing measures and technical safeguards are in place to prevent misuse of data?

All privileged role holders within ACS must meet qualifications and sign special Rules of Behavior for Trusted Persons that is periodically renewed. Private Key recovery requires a minimum of two authorized administrators with administrator certificates and key recovery privilege. Defined system security events trigger e-mail alerts. Viewing audit data requires administrator privileges.

7. Are the data secured in accordance with FISMA requirements?

Yes.

- a. If yes, when was Certification and Accreditation last completed?

July 21, 2008, ADAMS ML081850471. The system is currently going through an updated Certification and Accreditation for the major change to the system architecture.

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

System Name: Authentication and Credentialing Services (ACS) System

Submitting Office: Office of Information Services

A. PRIVACY ACT APPLICABILITY REVIEW

Privacy Act is not applicable.

Privacy Act is applicable.

Comments:

ACS is maintained as part of NRC's Privacy Act System of Records NRC-45, Digital Certificates for Personal Identity Verification Records. ACS maintains personally identifiable information.

Reviewer's Name	Title	Date
Sandra S. Northern	Privacy Act Program Analyst	September 17, 2009

B. INFORMATION COLLECTION APPLICABILITY DETERMINATION

No OMB clearance is needed.

OMB clearance is needed.

Currently has OMB Clearance. Clearance No. _____

Comments:

The information collected under the Authentication and Credentialing System is considered a certification under the Paperwork Reduction Act of 1995 (PRA), and is used to identify an individual in a routine, non-intrusive, non-burdensome way. Inquiries which certify the identity of an individual in a non-intrusive way are not considered an information collection under PRA, so no OMB clearance is required.

Reviewer's Name	Title	Date
Tremaine Donnell	Information Collections Team Leader	09/21/2009

C. RECORDS RETENTION AND DISPOSAL SCHEDULE DETERMINATION

- No record schedule required.
- Additional information is needed to complete assessment.
- Needs to be scheduled.
- Existing records retention and disposition schedule covers the system - no modifications needed.
- Records retention and disposition schedule has been submitted to the National Archives and Records Administration (NARA) and is **pending**.

Comments:

Many of the issues raised in the previous PIA (ADAMS ML060580656) were considered in this one. One such issue that remains is the fact that the retentions will be dictated by those approved in the pending schedule. Nevertheless, the fact that the schedule remains open or pending at NARA should not prevent the certification of this system.

Reviewer's Name	Title	Date
Mary L. Haynes	Records Management Analyst	09/18/09

D. BRANCH CHIEF REVIEW AND CONCURRENCE

- This IT system **does not** collect, maintain, or disseminate information in identifiable form from or about members of the* public.
- This IT system **does** collect, maintain, or disseminate information in identifiable form from or about members of the public.

I concur in the Privacy Act, Information Collections, and Records Management reviews:

/RAN/
 Russell A. Nichols, Chief
 Records and FOIA/Privacy Services Branch
 Information and Records Services Division
 Office of Information Services

Date: 09/21/2009

**TRANSMITTAL OF PRIVACY IMPACT ASSESSMENT/
PRIVACY IMPACT ASSESSMENT REVIEW RESULTS**

TO: Thomas W. Rich, Director, Infrastructure and Computer Operations Division, Office of Information Services	
Name of System: Authentication and Credentialing Services	
Date RFPSB received PIA for review: September 3, 2009	Date RFPSB completed PIA review: September 21, 2009
<p>Noted Issues:</p> <p>ACS is maintained as part of NRC's Privacy Act System of Records NRC-45, Digital Certificates for Personal Identity Verification Records.</p> <p>ACS maintains personally identifiable information.</p> <p>No information collection issues – no OMB approval required.</p> <p>Records retention and disposition schedule approval pending from NARA.</p>	
Russell A. Nichols, Chief Records and FOIA/Privacy Services Branch Office of Information Services	Signature/Date: /RAN/ 09/21/2009
<p><i>Copies of this PIA will be provided to:</i></p> <p><i>James Shields, Acting Director Business Process Improvement and Applications Division Office of Information Services</i></p> <p><i>Paul Ricketts Senior IT Security Officer (SITSO) FISMA Compliance and Oversight Team Computer Security Office</i></p>	