



E-AUTHENTICATION

SMART CARD

LOGICAL ACCESS & E-SIGNATURE

PRIVACY IMPACT ASSESSMENT

MAY 17, 2004
WO-850

UNITED STATES DEPARTMENT OF THE INTERIOR
WASHINGTON, D.C.

SECTION I

Department of the Interior Privacy Impact Assessment

Once completed please provide copies of the PIA to the following:

- Bureau/office IT Security Manager (when a C&A is required)
- Bureau/office Privacy Act Officer
- Office of Management and Budget (OMB) Capital Planning Exhibit 300 Submission (when an Exhibit 300 is required).

Also refer to the signature approval page at the end of this document.

A. CONTACT INFORMATION:

- 1) **Who is the person completing this document?** (*Name, title, organization and contact information*).

Bob Donelson,
DOI Representative to OMB for Electronic Signature
Senior Property Management Specialist (WO-850)
MS 1075 LS
1849 C St., NW, Washington, DC 20240

- 2) **Who is the system owner?** (*Name, organization and contact information*).

Hord Tipton
Chief Information Officer
U.S. Department of the Interior
1849 C Street, N.W.
Washington, D.C. 20240

- 3) **Who is the system manager for this system or application?** (*Name, organization, and contact information*).

Scott MacPherson
Information Resources Management Center Director
Bureau of Land Management
Denver Federal Center, Building 40
P.O. Box 25047
Denver, Colorado 80225-0047

Smart Card – Logical Access & E-Signature

- 4) **Who is the IT Security Manager who reviewed this document?** (*Name, organization, and contact information*).

David Cavallier
Installation Information Technology Security Manager
Bureau of Land Management (NI-160)
Denver Federal Center, Bldg. 40
P.O. Box 25047
Denver, Colorado 80225-0047

- 5) **Who is the Bureau/Office Privacy Act Officer who reviewed this document?** (*Name, organization, and contact information*).

John Livornese
Privacy Act Officer
Bureau of Land Management (WO-560)
1849 C Street, N.W., MS 725 LS
Washington, D.C. 20240

- 6) **Who is the Reviewing Official ?**

Ronnie Levine
Chief Information Officer
Bureau of Land Management (WO-500)
MIB - Room 5627
1849 C Street, N.W.
Washington, D.C. 20240

B. SYSTEM APPLICATION/GENERAL INFORMATION:

- 1) **Does this system contain any personal information about individuals?**

Yes

- a. **Is this information identifiable to the individual¹?**

Yes

¹ "Identifiable Form" - According to the OMB Memo M-03-22, this means information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors).

Smart Card – Logical Access & E-Signature

b. Is the information about individual members of the public?

(If YES, a PIA must be submitted with the OMB Exhibit 300, and with the IT Security C&A documentation).

No.

c. Is the information about employees? (If yes and there is no information about members of the public, the PIA is required for the DOI IT Security C&A process, but is not required to be submitted with the OMB Exhibit 300 documentation).

Yes.

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

The primary purposes of the system are:

- (1) To ensure the security of DOI computer networks to maintain continuous communications and protect the information attached to the networks from unauthorized access, tampering or destruction;
- (2) To verify that all persons accessing DOI networks with smart card systems are authorized to access them;
- (2) To ensure that persons signing official documents are indeed the person represented and to provide for non-repudiation of the use of an electronic signature; and
- (3) To enable an individual to encrypt and decrypt documents for secure transmission.

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

5 U.S.C. 301; Presidential Memorandum on Upgrading Security at Federal Facilities, June 28, 1995.

Federal Information Security Act (P.L. 104-106), Section 5113.

E-Government Act (P.L. 104-347), Section 203.

C. DATA in the SYSTEM:

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

Records are maintained on current agency employees, former agency employees, and agency contractors, volunteers and members of cooperating organizations who seek access to the DOI computer network or systems including the filing of forms that require an electronic signature.

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?**

The Information contained in the database is derived from individuals applying for a verifiable electronic signature certificate or access to a DOI computer network or system covered by this access control system, supervisors, and designated approving officials.

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

The Department of the Interior including its Offices and Bureaus will input the data provided by the individual.

- c. What Tribal, State and 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?**

The Microsoft Active Directory, is the repository for the system data. A contracted certification authority (currently VeriSign inc.) provides the digital certificate and encryption services necessary for secure authentication and verification. The collected data will contain the individual's User ID/email address. The System will also contain the individual's personal identification security card serial number and generates the date of entry to the computer network/system, time of entry, location of entry, time of exit, security access category, and access status. The collected data may also contain; office telephone number, supervisor's name, web home page address.

The Smart card logical access chip contains the digital certificate, date of issuance, expiration date, and the user's User ID/email address. The digital certificate is an encrypted field that contains no intelligible data. It is only a means of providing authentication. Only the user's User ID/email address links the user to the certificate.

3) Accuracy, Timeliness, and Reliability

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

We will accept the certification of accuracy, provided by the sender, of the information collected.

- b. How will data be checked for completeness?**

When it is brought to our attention that the data are incomplete we will contact the person or supplying agency for the missing data.

- c. Is the data current? (What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (e.g., data models)).**

Data are updated when employment status change. Agency clearance forms will trigger the necessary changes.

- d. Are the data elements described in detail and documented? (If yes, what is the name of the document?)**

Yes. They are described in Microsoft Active Directory Services user guide.

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?**

No. This information is the same information that was collected by the previous access control system which relied on the entry of a user ID and password. In this system, the user ID and password are replaced with an encrypted certificate on a smart card and a personal identification number (PIN).

- 3) Will the new data be placed in the individual's record?**

Smart Card – Logical Access & E-Signature

N/A

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

N/A

- 5) How will the new data be verified for relevance and accuracy?**

N/A

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

N/A

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

The user's access to the data will be limited by the access rights that are assigned to their password. The IT security staff will be able to add/delete records, search the data base for particular items, print reports, and grant/deny access to specific computer systems.

- 8) How will the data be retrieved? (*Does a personal identifier retrieve the data? If yes, explain and list the identifiers that will be used to retrieve information on the individual.*)**

Records are retrievable by name, User ID/email address, organization/office of assignment, security access category, date of entry to the network/system, time of entry, location of entry, time of exit, and ID security card serial number.

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

The Active Directory (AD) portion of this system of records has the ability to produce a variety of reports that can show system activity, system history, card holder activity, and card holder access rights. The certification issuance portion of this system of records is restricted to certificate controlled access and can only generate reports about the cards and the assignments of cards and about the certifications, not about the use after they are issued. The reports from AD can be used to determine which users have access to certain systems, who has accessed particular computer systems, etc. Access to the AD report functions is password protected and limited to internal system

Smart Card – Logical Access & E-Signature

administrators and security personnel involved in the routine operation of the system, except as noted below.

Disclosures outside the Department of the Interior may be made:

- (1) To security services companies that provide monitoring and maintenance support for the system.
- (2) To the Federal Protective Service and appropriate Federal, State, and local law enforcement agencies to investigate emergency response situations or to investigate and prosecute the violation of law, statute, rule, regulation, order, or license.
- (3) To the U.S. Department of Justice or to a court or adjudicative body with jurisdiction when (a) the United States, the Department of the Interior, or, when represented by the government, an employee of the Department is a party to litigation of anticipated litigation of has an interest in such litigation, and (b) the Department of the Interior determines that the disclosure is relevant or necessary to the litigation and is compatible with the purpose for which the records were compiled.
- (4) To a congressional office in connection with an inquiry an individual covered by the system has made to the congressional office.
- (5) To representatives of the General Services Administration or the National Archives and Records Administration to conduct records management inspections under the authority of 44 U.S.C. 2903 and 2904.

10) What opportunities do individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent.)

The information the individual provides is required before a certificate is issued. The certificate enables the holder to perform key tasks that may be necessary for the individual to perform duties required of their employment. If those duties are not required by their employment, the individual may decline a certificate.

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?

Active Directory access granted to individuals is password-protected. Access to the certificate issuance portion of this system of records is controlled by a digital certificate in combination with a personal identification number (PIN).

Smart Card – Logical Access & E-Signature

In both cases, each person granted access to the system must be trained and individually authorized to use the system. All system users are required to follow established internal security protocols.

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

Records relating to persons covered by this system are retained in accordance with General Records Schedule 18, Item No. 17. Unless retained for specific, ongoing security investigations:

- (1) Records relating to individuals other than employees are destroyed two years after ID security card expiration date.
- (2) Records relating to date and time of entry and exit for the computer network/systems by employees are destroyed two years after date of entry and exit.
- (3) All other records relating to employees are destroyed two years after expiration date of the digital certificate.

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?

Computer records of individuals will be deleted from the system in accordance with the records retention period listed above. Printed records will be handled according to the Department of the Interior General Records Schedule 18, dated June 1988 under the section of Security and Protective Services Records. An SF-115 is being submitted to the National Archives and Records Administration for approval.

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

This system will use smart cards for access to DOI computer networks and systems. Smart cards using various proprietary standards are currently implemented in the DOI at a number of locations. This system will implement a single technical standard and expand its use throughout the DOI.

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

This system will be used to control, and may be used to monitor, entry/exit to DOI computer networks and systems by card holders.

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

Yes. The AD portion of this system of records will record the entry/exit to DOI computer networks and systems by card holders.

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

The location and time of entry/exit to Department of the Interior computer networks and systems will be recorded in the AD portion of this system of records. The date and time of signing of forms or documents requiring the use of the electronic signature digital certificate will be recorded.

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

Access for AD granted to individuals is password-protected at the present time and will be accessible only by use of a certificate and PIN in the future. Access to the certification issuance portion of this system of records is accessible only by use of a certificate and PIN. Each person granted access to the system at must be trained and individually authorized to access the system. All system users are required to follow established internal security protocols. Performance of contract employees is monitored.

9) Under which Privacy Act systems of records notice does the system operate? Provide number and name.

No Privacy Act Notice currently exists. A new Federal Register Notice is currently in surname and is expected to be published by the end of June, 2004.

10) If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.

N/A

F. ACCESS TO DATA:

1) Who will have access to the data in the system? (E.g., contractors, users, managers, system administrators, developers, tribes, other)

Secure access to data covered by this system is available at all locations within Department of the Interior where IT System Administrators and IT Security staff have been authorized access to the data.

2) How is access to the data by a user determined? (Are criteria, procedures, controls, and responsibilities regarding access documented?)

Smart Card – Logical Access & E-Signature

Access granted to individuals is either password-protected or protected by the use of secure digital certificates in combination with a personal identification number (PIN); each person granted access to the system must be individually authorized to use the system.

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

The individual user will not have access to the data. The IT System Administrator, with the approval of the IT Security Manager, will be able to add/delete records, search the data base for particular items, print reports, and grant/deny access to specific systems. Data access is limited by "access roles" defined during the set-up of the operator

- 4) What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access? (Please list processes and training materials)**

Access to AD is password-protected. Access to the certificate issuing system is protected by the use of secure digital certificates in combination with a PIN; each person granted access to the system must be trained and individually authorized to use the system. All system users are required to follow established internal security protocols. Performance of contract employees is monitored.

- 5) Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? (If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed?)**

Yes, A Privacy Act clause is in the contract.

- 6) Do other systems share data or have access to the data in the system? If yes, explain.**

No other system shares data in the system; nor does any other system have access to the data in the system.

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

The designated System Manager.

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

Smart Card – Logical Access & E-Signature

Access is limited to System Administrators and IT Security Officers in the Department of the Interior and to those identified in the Privacy Act System of records and according to the Privacy Act.

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

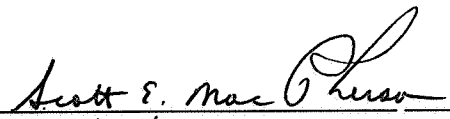
N/A

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

The Department of the Interior, IT Security Manager.

The Following Officials Have Approved this Document

1) System Manager

 (Signature)
05/17/04

Name Scott MacPherson

Title Director,
National Information Resources Management Center, BLM


2) IT Security Manager

 (Signature)

Name Dave Cavallier

Title IT Security Manager, BLM National IRM Center


3) Privacy Act Officer

 (Signature)

Name John Livornese

Title Privacy Act Officer, BLM

4) Reviewing Official

Acting CIO  5/24/04 (Signature)

Name Ronnie Levine

Title Chief Information Officer, BLM