




# United States Department of the Interior

OFFICE OF THE SECRETARY  
Washington, D.C. 20240

**OCIO DIRECTIVE 2004 - 008**

**FEB 19 2004**

To: Heads of Bureaus and Offices

From: W. Hord Tipton  
Chief Information Officer 

Subject: Credentialing Activity Standards & Smart Card Acquisition Requirements

**Purpose:**

This directive provides policy and guidance on Credentialing Activity Standards & Smart Card Acquisition Requirements.

**Background:**

The President's Management Agenda of 2000 is the cornerstone of the Administration's goal of making government citizen-centered through the expansion of electronic government (E-Gov). In an effort to reduce the burden to citizens, businesses, and government, E-Gov initiatives established by the President's Management Council are transforming government operations in order to improve effectiveness, efficiency, and service delivery. Providing E-Gov services is a complex process cutting across programs throughout the Department of the Interior (DOI).

One of the critical components of the E-Gov initiative is authentication. Authentication is the process of determining with certainty that someone really is who they claim to be. The process of authenticating an individual involves establishing the individual's unique identity or establishing that the individual is a member of a group, such as a military veteran or U.S. citizen. Federal Identity Credentialing (FIC) provides a secure process for authenticating users for access to federal resources such as computer systems and buildings.

Establishing the DOI E-Authentication capability will employ a three tier approach:

- Tier one activity will include the establishment of secure FIC, access controls and authentication of DOI facilities, information systems, and networks supporting requirements outlined in the Federal Information Security Management Act of 2002.
- Tier two activity will include establishing a secure public key infrastructure (PKI) framework for application access to improve the security posture of DOI's most sensitive systems.

- Tier three will leverage PKI to provide digital signatures for more efficient and secure document creation, exchange, and management meeting mandates outlined in the Government Paperwork Elimination Act.

**Scope:**

This directive applies to all DOI offices and bureaus.

**Policy:**

**Issuance of Smart Card Credential Badge**

In accordance with Federal E-Authentication requirements, DOI needs to issue a smart card credential badge, herein referred to as a FIC, to all DOI employees and its trusted agents. The purpose of this directive is to provide guidance to support planning for identity and credentialing investments, specifically related to smart card badging for DOI. This will lead to a robust identity and authentication platform for non-repudiation of transactions for both physical and logical access. Successful planning and implementation in this area will require the support of all DOI staff involved in credentialing and identification, including those involved in physical and cyber security, human resources, system, and network administration. The primary intent is to eliminate inconsistent approaches to both physical and computer security, which lead to increased risks to DOI. It should be noted that DOI has considerable experience in the FIC area due to the work carried out by the Bureau of Land Management (BLM) over the past two years. The BLM Smart Card implementation is considered a best practice and is being utilized to shape E-Authentication policy and standards across the government and DOI.

**Smart Card Acquisition Requirements**

Effective immediately, a freeze is placed on all purchasing and deployment activities associated with FIC that are not in compliance with E-Authentication requirements outlined below. This freeze is applicable to employee and contractor badges, smart cards, smart card readers, card management systems, associated software known as smart card middleware, and computer hardware.

- All future acquisitions within DOI must meet Government Smart Card specifications as outlined by the FIC project of the E-authentication initiative located at <http://www.cio.gov/ficc>.
- All future Physical Access Systems must contain Government Smart Card Interoperability Specification Version 2.1 (GSCisV2.1) readers located at <http://smartcard.nist.gov/>.
- All current and future computer purchases must acquire GSCisV2.1 compliant Smart Card readers on keyboards as part of the procurement. DOI's hardware Blanket Purchase Agreement (BPA) awarded to Dell has been recently modified

to include these keyboards as part of the contract. Buyers can obtain additional information by logging on to the following website:  
<http://www.doi.gov/ocio/erm/hardware/index.html>.

- The Department Smart Card/PKI steering committee is analyzing the costs associated with choosing either a Universal Serial Bus or Personal Computer Memory Card International Association Smart Card reader for laptop computers. Once the decision is made the committee will work to have the appropriate Smart Card reader added to DOI's hardware BPA.
- All Smart Cards for the Department must be purchased through the consolidated Government Smart Card process. Please contact Bob Donelson, BLM Senior Property Manager Specialist, at [Bob\\_Donelson@blm.gov](mailto:Bob_Donelson@blm.gov) or by phone at (202) 452-5190 for additional information.
- The transport keys on the Smart Cards must meet the issuance specification developed between DOI, Department of Defense, and the General Services Administration to securely integrate into DOI's Card Management System. Please contact Bob Donelson for additional information.
- Each Bureau is to establish an integrated implementation team to collaborate with the Department to fully realize the goals of the E-Authentication project.
- Bureaus are to provide the names of their implementation team members, plan and relevant standards documentation to the DOI Chief Information Officer by June 30, 2004. If no plan or standards exist at this time, please provide team members only.

If you have any questions concerning this directive, please contact me at (202) 208-6194. Staff may contact Roger Mahach, the DOI IT Security Manager, at the same number. Bob Donelson, the BLM Smart Card Program Manager, may be contacted at (202) 452-5190.

cc: Bureau Chief Information Officers  
Bureau Information Technology Security Managers  
Interior Architecture Working Group