

Guidance Regarding Smart Cards Systems For Identification and Credentialing of Employees

A. Background

On July 3, 2003, OMB released a policy memorandum titled “Streamlining Authentication and Identity Management within the Federal Government.”¹ The memorandum announced the creation of the Federal Identity and Credentialing Committee who would be charged with developing a “common, comprehensive policy for the credentialing of Federal employees.” Agency Chief Information Officers were interested in eliminating inconsistent approaches to the credentialing of Federal employees and redundant costs to the Federal government and the people with whom it interacts.

This is the first in a series of documents, designed to put forth guidance on those Federal agencies that choose to implement smart card² systems for the identification and credential of their employees, contractors and other authorized individuals.

B. Purpose and Applicability

This document provides guidance on the use of smart card based technology in badge, identification, and credentialing systems within the Federal sector, with the objective of helping agencies plan, budget, establish and implement credentialing and identification systems for Federal government employees and their agents. This document applies specifically to the use of smart card based platforms in the credentialing and identification activities of Federal government employees, contractors and affiliates supporting Federal agencies and includes a migration path to incorporating logical access capability.

Following the guidance set forth in this document will lead to a robust, interoperable identity and authentication platform both for physical facility and logical access conducted on sensitive but unclassified networks. Successful agency planning and implementation requires the support of all the Agency communities involved in credentialing and identification, including those involved in physical and cyber security, human resources management, and identity management.

Agencies who implement this guidance will issue identity credentials (smart cards) within its own domain in a secure manner to assure that each credential issued is bound to a person whose identity has been carefully vetted. Although issued individually by each agency, the end result will be a “trusted token” that can be made interoperable across the entire Federal enterprise. Interoperability includes the ability to have an individual’s identity electronically

¹ OMB Memorandum, 7/3/03, <http://www.whitehouse.gov/omb/inforeg/eauth.pdf>

² Smart cards are plastic devices—about the size of a credit card—that use integrated circuit chips to store and process data, much like a computer. This processing capability distinguishes these cards from traditional magnetic stripe cards, which cannot process or exchange data with automated information systems.

verified within the agency domain and across the federal enterprise for both physical and logical networks. The smart card-based identity credential will be the token used to establish (electronically read) an individual's identity and provide the functionality for authentication of that person when challenged or required.

This guidance does not apply to those systems that are national security systems as defined in U.S.C. 3542(b)(2). This guidance does not apply directly to authorization but to using a smart card platform capable of authentication and interoperability with other smart card-based systems. Decisions concerning authorization remain the purview of agencies and responsible security and facility officials. Authorization focuses on the actions permitted of an identity after authentication has taken place. This guidance encourages (but does not require) the use of smart cards for both physical and logical access, and emphasizes them for badge systems, whose primary purpose is for identification of employees and entry to Federal facilities and networks.

C. Robust Interoperable Identification Platform

Implementation of this guidance requires that Federal agencies begin planning for the migration of their current access control systems, both physical and logical. Agencies should:

- Establish the issuance and deployment of an electronically readable credentialing smart card as the platform of choice for identity and authentication. For the purpose of this policy, the platform of choice will be a smart card that contains a contact and contactless integrated circuit chip. At the direction of the agency and in the short term, the platform may also incorporate other technologies on the card platform, as required to support legacy systems (e.g., magnetic stripe, bar code)
- Adopt standards for smart card and credentialing implementation that will permit interoperability of the smart card across all agency components as well as the entire Federal enterprise.
- Plan for a higher threshold for credentialing employees and agents. This threshold should exceed existing credentialing systems today, which are based on a flash pass or card with, at most, PIN-based verification. A more robust credentialing functionality allows agencies to meet the need for identity and authentication for various threat levels and in disparate building and network infrastructures. This implies authentication methods beyond passwords for authentication to logical networks/applications, and methods beyond non-electronically-readable photo verification for physical access. The methods should include an active means of authentication for verification before access permissions are granted.
- Provide direction to component bureaus and entities requiring them to plan and budget based on principles of enterprise-wide implementation, use of standards-based systems components and interoperability. Such direction will help to maximize

competition, minimize infrastructure costs, enable enterprise-wide interoperability of credentials, and improve security.

- Adopt practices that will ensure privacy while improving credentialing systems to improve security and promote efficiency of government business operations using standards-based technology. In the interest of protecting privacy of individuals, practices will also bar efforts to develop, or expand, existing databases for the purpose of tracking employee activity.

D. The Intent of Interoperability and Setting the “Trust Model”

The intent for an interoperable, smart card-based Federal Agency Smart Credential (FASC) is to grant the attributes of “identity and a basic level of authentication” to a commonly accepted card across the Federal enterprise of sensitive but unclassified networks. As always, privileges granted to the bearer of the FASC is a local agency matter. The FASC is a core component to setting the “trust model” for these stated networks across the entire federal enterprise. It is intended that back end databases be updated to accept the credentials contained in the FASC. Agencies may invoke additional degrees of authentication beyond the FASC, as they deem appropriate for access control and liability purposes.

The FASC is to be used as the identity and basic authentication credential before an individual may gain access privileges for work-related and agency approved responsibilities within the *Issuing Agency*. It will be the basis of identity and basic authentication when visiting other domains within the federal government enterprise. It is intended that outside the issuing agency domain the FASC be recognized as the basis for identity and basic authentication by the *Relying Agency* and be the basis for granting access privileges without issuance of another identity card. The relying agency has the responsibility to verify the identity and validity status of the bearer of the FASC with the issuing agency as appropriate. The relying agency may issue additional logical credentials to the FASC issued by another agency if deemed necessary, but is required to seek approval of the issuing agency.

E. Binding the Identity to the FASC at Issuance

Issuance of the Federal Agency Smart Credential requires verification of end user identity prior to issuance. Each agency will employ an identity verification program prior to issuance of the FASC. The FASC will be acquired and issued in a secure process by the issuing agency that will include “In Person Proofing” that binds the “verified identity” of the intended bearer of the FASC to the credentials issued by the agency. The agency process will require that the bearer present source documentation, referred to as ‘breeder documentation, that will be verified and validated by the issuing agency in an in-person process prior to issuance of the FASC. The quantity and detail of breeder documentation required before issuance is agency dependent. Background investigations of criminal history, education certifications, credit history, work history, and so forth is at the discretion of each agency but at a minimum must meet current Office of Personnel Management (for

Government employees) and Federal Acquisition Regulation (for contract agents) regulations.

To the extent that the authentication process captures information that is protected by the Privacy Act (because it is information about an individual that the agency retrieves by an individual's name or other identifier and thus is maintained in an agency Privacy Act system of records), the agency needs to comply with the Privacy Act with respect to such information.

F. Agency Planning

Agencies should establish a smart card based identity and credentialing framework that:

- Assures that Federal suitability investigations are undertaken for all employees and contractors in accordance with Federal law and policy.
- Adopts a clear and concise definition of terms so that all agencies have a common understanding and criteria for the trust model implemented by the issuing agency.
- Drives trust of multi-agency credential tokens and credential information across the defined enterprise infrastructure. The system design must include a federated environment in order to determine with a high degree of confidence the identity, affiliated organization and credential entitlement of the guest credential (a credential presented from outside the agency). A federated approach takes into account how to deal with credential and token bearers from other issuers outside the facility being accessed.
- Is driven by both Federal enterprise requirements as well as individual agency needs and includes recognition of the total cost of an access infrastructure for both physical and logical access. To maintain a common understanding of the latest developments, agencies are encouraged to participate in the scheduled meetings of the Federal Identity and Credentialing Committee (see www.cio.gov/ficc), the Smart Card Project Managers meetings, and the Smart Card Interagency Advisory Board (IAB) (see www.smart.gov).
- Converges disparate identity and authentication identity badges and other media to a common credential smart card used and trusted across the defined enterprise.
- Is flexible enough to meet additional agency needs using legacy tokens until such time legacy systems are replaced and upgraded.
- Safeguards individual rights to privacy.

G. Common Credential Requirements for Smart Cards

Minimum requirements follow:

- Identity data must be in a standard electronically readable format and use an active authentication process.
- Information contained both on the visible surface of the Federal Agency Smart Credential and within the chips will be tamper resistant and counterfeit-resistant. A tamper-resistant card contains features both making it difficult for persons to alter the information, and making alterations readily apparent to a qualified person or validating system. A counterfeit-resistant smart card contains features making it difficult for persons to produce illegitimate tokens that could be incorrectly accepted by a qualified person or validating system.
- Cards should support multiple authentication methods to protect the credential token from unauthorized use or theft. Factors may include something you know (e.g., a password), something you have in your possession (e.g., a digital certificate), and something you are (e.g., a biometric such as a fingerprint or iris scan). Agencies are encouraged to provide support for all these methods and associated technologies in their architecture and planning.
- Smart cards must be supported by an infrastructure providing automated administration and maintenance of audit trails of smart card usage and must be in accordance with Electronic Records Management systems requirements.
- Every smart card should have the capability to carry digital certificates for identity, encryption and digital signature. Credential requirements should be standards based meeting the certification requirements of the Federal Bridge model including all NIST recommended and approved standards and specifications such as FIPS 140-2: Security Requirements for Cryptographic Modules.
- Cards should have the capability to carry certificates needed to sign and encrypt sensitive mail as defined by the agency and be supported by agency applications.
- The card should allow post-issuance updating of data in a secure fashion and using a multi-factor means of authentication.
- The card should comply with NISTIR 6887, 2003 Edition – *Government Smart Card Interoperability Specification v2.1* (and later versions as they are issued) – identification formal standards, and other standards as appropriate.
- Applications ported to the Federal Agency Smart Credential will be subjected to a certification process to ensure they are downloaded to the card in a secure and trusted manner and may require FIPS 140-2 validation. All applications or data downloaded to the Federal Agency Smart Credential are the responsibility of the issuing agency both at initial issuance and post issuance.

- For security purposes agencies need to establish and enforce work policies and business processes that report a stolen or lost Federal Agency Smart Credential and revocation of privileges based on the Federal Agency Smart Credential as soon as possible. Agencies will also need to enter into agreements with other cooperating entities on procedures and methods to be developed for cross-agency notification when a credential is revoked or suspended.

H. Life Cycle Requirements

Agencies should plan for the entire life cycle of smart card based platforms, including the following functional components:

- Identity vetting – Identity vetting involves in-person proofing, and verification of authenticity and validity of breeder documentation. Identity vetting includes a process used to verify the identity of an individual via direct face-to-face validation of claimed identities and/or linkage to an authentication method. To assure identity in a trusted environment, agencies must address the specific issues of identity proofing and identity validation based on valid supporting documentation and, where possible, via the electronic verification and validation of the bearer’s breeder documents (e.g., birth certificates and other basic documents user to obtain commonly obtained identity documents).
- Enrollment and registration – Enrollment is the process used to publish that a vetted individual has been sponsored by an organization. Once the individual’s identity has been verified to an agreed upon assurance level, the individual will report to an enrollment station where a trusted agent will review that the individual’s request has been processed correctly and completely. Registration is the process used to enter a vetted and enrolled individual into a security system and/or associated database. Agencies must develop policies that control and define the enrollment and registration processes.
- Card issuance – Card issuance is the process of distributing personalized cards to cardholders. Personalization entails both the logical and physical personalization of the card. Logical personalization involves transmittal and injection of the appropriate card applications, credentials, data, PIN and biometrics into the card application. Physical personalization encompasses printing of the physical characteristics and security features on the surface of the card. The personalization process is protected by controlled and highly secure methods. Agencies must develop policy guidance for card-processing requirements of initialization, personalization and fulfillment steps of card issuance based on applicable ISO, ANSI, FIPS, and NIST standards and interoperability specifications.
- Card usage – The smart card is one of the most efficient authentication devices that can be used for both physical and logical access control applications. The smart card

supports federated identity concepts, has trust characteristics that enable verification and validation of the integrity of credentials, and supports the OMB E-Authentication Guidance for Federal Agencies³. Agencies must provide policy guidance of how the card itself and credentials it stores can be used to provide necessary authentication levels for the access control of government facilities and services.

- Card revocation – For both physical and logical access controls, agencies must provide policy guidance of managing revocation of the card itself and credentials it stores.
- Post issuance updates or additions – Multi-application smart cards need to provide capabilities to add, delete and update card applications or data elements during the post-issuance phase of card life cycle. Agencies must define card configuration management and delegation of authority policies governing the creation, deletion, transfer and instantiation of card applications.
- Card reissuance and termination – The card reissuance process is used to provide replacements to individuals reporting a lost, stolen, or malfunctioning card. Generally when the card is reported lost, stolen, or malfunctioning, customer service deactivates the card by placing it on a list of cards that should not be honored if presented in the future. When a replacement card is issued, it must carry all the privileges, data, or and system access keys that resided on the original card that is being replaced. The termination process is used to permanently destroy or invalidate the usage of the card. Agencies must provide policy guidance for these processes.

Agencies should plan for a functional card life of up to six years.

I. Card Data Models

For smart card systems to work interoperably, it is important that agencies use common data models in a specified value format so that all Federal Agency Smart Credentials issued have the ability to be used throughout the federal enterprise, not just the agency's issuing domain. Agencies should be compliant with card data models defined in the most recent issuance of the *NISTIR 6887 – 2003 Edition, Government Smart Card Interoperability Specification (GSC-IS) v2.1*. It is at the discretion of each agency to select a data model for implementation before issuance. In accordance with the GSC-IS, the card capability container and an access control file for physical access is mandatory regardless of the data model selected. At this writing, agencies are working with the Government Smart Card Interagency Advisory Board (IAB) to develop a common minimum data model for use throughout the Federal enterprise.

J. Risk and Security Considerations

³ OMB Memorandum M-04-04, 12/16/03, <http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf>

NIST is finalizing SP 800-63 “Recommendation for Electronic Authentication” which will recommend technology solutions for four assurance levels for electronic transactions. Smart card systems must be developed to meet the requirements of this Special Publication. Physical security managers also need to develop risk-based approaches for badging policies related to physical access. Federal buildings are currently classified in four different categories, based on level or risk associated with attacks on buildings. Smart card systems should be considered for earlier implementation for facilities in the highest risk categories.

K. Biometric Technology

Agencies should design smart card systems that that are robust enough to support biometrics for current or future applications. Biometrics adopted for use on smart cards must adhere to standards set by the American National Standards Institute (ANSI), InterNational Committee for Information Technology Standards (INCITS), the International Organization for Standardization (ISO), and the National Institute of Standards and Technology (NIST).