

Authentication and Identity Policy Framework For Federal Agencies

The following document presents a direction for Federal Identity Credentialing. In many cases the document may appear to be prescriptive and to levy mandatory requirements on Federal agencies. This document does not bear the authority to make such requirements or to enforce them, however, it is laying out a framework, or roadmap, for moving toward a government-wide standardization of Federal Identity Credentialing, the success of which may result in mandatory compliance.

1. Purpose

The Authentication and Identity Policy Framework for Federal Agencies defines the activities of the Federal Identity Credentialing Committee (FICC), under the authority of the Federal CIO Council, as provided for by the E-Government Act of 2002. This framework is not intended to address national security systems, as defined in 44 U.S.C. 3545(b)(2).

E-Government, an integral part of the President's Management Agenda (PMA), is defined as the use of digital technologies to transform government operations in order to improve effectiveness, efficiency, and service delivery. As the Federal government modernizes internal processes and adopts cross-agency applications available to all Federal employees, a common, trusted basis for authenticating the identity of individuals within the Federal sector is required. This policy framework document is designed to outline a successful approach to providing the needed authentication services and it declares the following high-level objectives:

- Simplify and Unify Identity Authentication for Federal Employees.
- Define technical and policy requirements for physical access credentials, electronic credentials, and the issuance and management of such credentials.
- Provide a rational, common approach to authentication and identity for Federal employees.
- Identify business process and technical requirements related to management, operational and technical controls for credential life cycle management.

This framework describes policies for issuing and managing physical and logical access credentials for Federal personnel, contractors and other affiliated personnel, and a standardized and integrated credentialing process that encompasses both physical access to facilities (buildings, compounds, military installations) and logical access to systems. By standardizing credentials across the Federal government, individual access control can be streamlined across multiple organizations and systems. Government cost savings can be achieved through standardization, shared services, and consolidated purchasing.

Successful implementation of this policy framework will enable the following:

- Common standards, controls and expectations that form the basis of mutual recognition of authentication and access credentials across government in a

- uniform manner, including Federal Identity Cards that support official government identification card requirements;
- Processes for standardizing physical and digital format, data elements and models, characteristics, components, visual presentation and appropriate use of authentication and access credentials;
 - Uniform, streamlined approach to automated building access, visit requests and authorization across the government;
 - Immediate identification and subsequent denial of access for those with revoked or suspended credentials;
 - Improved access to interagency electronic processes, such as e-payroll and e-travel;
 - Cross-organizational recognition and authentication of e-mail correspondents, digital signatures, and message integrity, including provisions for non-repudiation services.

The degrees to which these goals are achieved may serve as metrics to evaluate the ongoing performance of the Government in implementing a common, secure identity management strategy.

This framework shall result in a Federal Identity Credentialing Component in the Federal Enterprise Architecture for issuing consolidated physical and electronic access credentials for Federal personnel, contractors and affiliated personnel that shall provide sufficient assurance to satisfy most governmentwide application and physical access control requirements.

2. Background

Authentication is the process of establishing confidence in the truth or authenticity of a claim or assertion. For the purpose of this framework, authentication has two representations – individual authentication and system authentication.

Individual authentication refers to the process of establishing an understood level of confidence that an identifier represents a specific individual. The process of authenticating an individual may involve establishing the individual's unique identity (identity authentication) or establishing that the individual is a member of a group, such as a military veteran or U.S. citizen (attribute authentication).

System authentication has two separate interdependent components – identification and authentication. Identification is the means by which a user provides a claimed identity to the system. Authentication is the means of establishing the validity of a user's claimed identity to the system.

In the past, Federal agencies have used a variety of authentication and access approaches that span identification cards, and independent physical and electronic mechanisms to authenticate personnel. In general, these authentication and access approaches have been agency-specific and have not supported cross-agency use. This authentication and access

framework addresses measures required in order to ensure that Federal personnel and other authorized users may be granted access correctly to Federal facilities, networks, and services. This is achieved by establishing a consistent level of assurance of the identity of a user requesting access rights to Federal facilities and systems using an electronic credential, a common set of criteria for credential issuance, and broadly interoperable authentication services that support validation of the credentials when interacting with an e-government service (both as a client in a transaction and as a service provider).

In the context of Federal identity credentialing, authentication is the first step in the larger process of granting physical or logical access to a facility or e-government service, called “authorization.” Authentication focuses on establishing a person’s identity based on the reliability of the credential he or she offers, while authorization focuses on what actions that identity, as established, is permitted to take. This policy framework addresses the authentication of Federal government employees, government contract employees, and other affiliated personnel as a prerequisite to evaluation of authorization to access resources. Since authorization refers to an individual’s right to access a particular resource, it is the responsibility of each Federal organization to determine the appropriate level of access permitted based on the characteristics of the authenticated credential, to determine its requirements to issue authorizations in general, and to determine the issuance of individual authorizations to specific resources in particular.

3. Federal Identity Credentialing Overview

Following is an overview for Federal agencies of assumptions related to granting identification credentials to personnel and other authorized users of Federal facilities, systems, and services.

- Federal personnel require physical access credentials for common access to Federal facilities and resources. Such credentials must embody reasonable protections against misrepresentation by incorporating tamper resistant characteristics, and should serve as secure platforms for electronic credentials.
- Minimum requirements for Federal access credentials include the following:
 - The credential will support both physical and logical access;
 - The credential will be usable for identity authentication and electronic signature;
 - The credential will be usable and interoperable across the Federal government by implementing smart card technology that incorporates both contact-less and contact technology in accordance with the Government Smart Card Interoperability Specification (NISTIR 6887)
 - The credential will be portable;
 - The credential will be issued by a federal government agency
 - The credential will be unique to the person identified by it.

- Multi-functional dual interface smart cards represent the technology that best meets government-wide needs for physical access credentials, which may also serve as secure platforms for electronic credentials (hardware tokens), in accordance with standards and guidelines.
- Federal agencies will serve as the authorizing agents for issuing and managing access credentials to Federal personnel and other authorized individuals and entities.
- Physical/logical access credentials for Federal personnel and other authorized users of Federal facilities and services will meet a minimum identity assurance level, understood by all Federal organizations and deemed sufficient to meet generic Federal security requirements for e-government applications and access control. Agencies may exceed the minimum assurance level for credential issuance to their employees, as required to satisfy their mission requirements.
- The technology for electronic credentials that best meets the Federal Government's needs at this time is Public Key Infrastructure (PKI) digital certificates.
- The most secure means to issue digital certificate credentials is on a secure hardware token.
 - The strongest security is achieved by the use of hardware tokens to generate and store the private key, and to perform cryptographic computations so that the private signature/authentication key is never exposed outside of the security of the token;
 - Hardware tokens should be used to provide secure portability of electronic credentials.
- A common Federal PKI Certificate Policy facilitates deployment of common digital credentials within the Federal government.
 - The Common Federal PKI Certificate Policy will be administered by the Federal PKI Policy Authority;
 - Federal agencies that issue digital credentials using PKI must comply with this common policy. Where agencies have already instantiated PKIs and published policies for that purpose, those policies shall be comparable to the Common Policy. The Certificate Policies of Agency PKIs already cross-certified with the Federal Bridge CA at medium assurance or above are deemed comparable with the Common Policy.
 - The Common Federal PKI Certificate Policy meets Level 3 assurance as defined by the *E-Authentication Guidance for Federal Agencies*.

- Each Federal agency issuing digital credentials under the common policy must create a Certification Practices Statement (CPS) demonstrating how their implementation complies with the Common Federal PKI Certificate Policy.
- The Federal PKI Policy Authority will identify a set of managed PKI services whose procedures comply with the Common Federal PKI Certificate Policy. These managed services will be made available for agency use through government-wide acquisition vehicles.
- Agencies that have already deployed an Enterprise PKI for the issuance of credentials to their employees and have cross-certified with the Federal Bridge Certification Authority are considered compliant with the Common Federal PKI Certificate Policy. However, any new Enterprise PKI deployments will require justification via the OMB Budget Process.
- Requests for exception from these policy principles must be supported by an Exhibit 300 business case, which must be approved by OMB through the normal budget approval process.

4. Determining Access Authorization

Once identity has been established through the authentication of physical or logical access credentials, access authorization will depend on the individual agency's access control requirements. For physical access to facilities, Federal program managers must determine the sensitivity level of the facility and its physical access criteria. For logical access, Federal program managers must perform risk assessments of their E-Government business process requirements, for functionality and security through appropriate access control models and features on each system. Decisions will be based on how the identified potential impacts can be mitigated by the application/access control requirements to achieve an acceptable level of risk based on the nature of the information being protected.

The Federal Identity Credentialing Component will identify a minimum set of requirements for identity assurance of Federal employees. Each Federal organization must then determine to what extent this minimum level of assurance meets its requirements for access to its facilities, systems and services, and what additional measures, if any, must be taken in order to authorize access.

5. Federal Agency Identity Assurance

Federal agencies are responsible for authenticating the identity of employees, contractors and other authorized personnel to whom they issue credentials. Federal organizations may delegate the identity authentication function to other Federal organizations or to

trusted agents; however, delegation shall not result in a reduction of the identity authentication requirements. Therefore, agencies may implement auditing and accountability processes of these authentication processes at their discretion.

All individuals authenticated under this policy framework must appear in person to obtain credentials issued by their agencies. Identity authentication procedures verify the applicant's identity based on established Federal statute and guidance, and establish an evidentiary trail to support prosecution in the event of fraudulently obtained credentials.

The process for credential issuance shall be initiated only based on a formal request by authorized agency representatives. Agencies shall establish criteria identifying which agency representatives are designated to make such requests in a manner that is consistent with Federal policy and consistent with the business requirements of the organization. The request for credential issuance shall identify the applicant as a Federal employee, a contract employee, or other affiliate.

Each agency shall ensure that full life cycle management of identity is established, taking into account employee, contractor, and affiliate credential requirements. Where appropriate, this requirement and supporting agencies processes should be incorporated into contractor and affiliate agreements.

6. Federal PKI Policy Implementation

These implementation criteria apply to agencies deploying electronic credentials using PKI technology to control access by Federal employees, contractors and other agency affiliated personnel to physical and/or logical resources.

The Federal Identity Credentialing Committee (FICC) has developed a Common Federal PKI Certificate Policy for use by Federal organizations when deploying digital credentials to their employees, contractors and affiliates. The Federal PKI Policy Authority (FPKIPA), an interagency subcommittee of the FICC, manages the Common Federal PKI Certificate Policy.

Under this framework, it is the intention of the Federal government to centralize processes for deployment of PKI. Therefore, the FICC will implement a process for establishing, approval, and oversight of managed service providers operating under the Common Federal PKI Certificate Policy from which Federal organizations may acquire digital certificates. As far as possible, Federal organizations deploying PKI to Federal employees, contractors or associates shall use certificates issued by these managed service providers. Exceptions must be requested through the OMB budget process.

Managed service providers that issue certificates under the Common Federal PKI Certificate Policy must present Certification Practices Statements (CPS) and third party audit results indicating compliance with the provisions of the common policy to the FICC for approval. The FICC will forward the documentation to the Federal PKI Policy Authority for review and approval to ensure that it is consistent with the Common

Federal PKI Certificate Policy and it will review the compliance audit report to ensure that the Certification Authority is operating in compliance with its CPS.

Federal organizations whose business cases justify operation of their own Certification Authorities within the Common Policy Framework shall utilize the common Federal PKI Certificate Policy, and shall submit their CPS for review by the Federal PKI Policy Authority.

Agencies adopting the Common Federal PKI Certificate Policy to issue digital certificates to their staffs, whether issued from their own CA or utilizing a managed service, and whose CPSs are approved by the FPKIPA may become voting members of the FPKIPA in accordance with that entity's rules and procedures.

Federal organizations that are granted an exemption from the Common Policy Framework by OMB based on their business case, but who also require interoperability within the Federal domain, will utilize the Federal Bridge Certification Authority (FBCA) as their interoperability mechanism. These organizations must ensure compliance with the following policy framework requirements:

- Shall have a continuously approved Exhibit 300, approved by OMB, that represents the business case for any such Common Federal PKI Certificate Policy -independent deployment;
- Must develop Certificate Policies of their own in addition to a CPS;
- Must contract to have an independent third party compliance audit performed on their behalf; and
- Will achieve interoperability through cross-certification with the FBCA, which requires each entity to map policies in accordance with the published *U.S. Government Public Key Infrastructure Cross-Certification Methodology and Criteria*.

Agencies adopting the Common Federal PKI Certificate Policy may choose to have other Certificate Policies asserted in certificates issued to their employees, contractors or affiliates, provided those policies are not contradictory to the Common Federal PKI Certificate Policy.

Federal organizations operating Certification Authorities that are cross-certified with the FBCA at the Medium or High assurance level on the effective date of the policy are considered in compliance with the Common Federal PKI Certificate Policy and are consistent with this Common Policy Framework. These organizations may continue to operate their Certification Authorities in this manner as long as they can satisfy the requirements of the Common Federal PKI Certificate Policy and OMB continues to provide approval, or they may transition to operations under the federally managed service, as desired.

The FBCA will facilitate interoperability between the Federal PKI and other Enterprise PKI domains (e.g. states, foreign governments, academia, industry, etc.), when such

interoperability is deemed in the best interest of the Federal government. Such interoperability will further support the E-Government Initiatives by facilitating trusted transactions with other government entities, citizens and businesses. Interoperability will be established through policy mapping by the Federal PKI Policy Authority and cross-certification with the FBCA as detailed in the *U.S. Government Public Key Infrastructure Cross-Certification Methodology and Criteria*.

7. Federal Agency Smart Card Implementation

The Federal Identity Credentialing framework requires that Federal Identity Credentials be incorporated into a smart card form factor, as defined by the Federal Smart Card Policy. Federal deployments of smart cards shall meet a common set of functional criteria as defined by the Federal Smart Card Policy and related guidance (i.e. Government Smart Card Interoperability Specification (GSC-IS v.2.1)). Such smart cards will be used as official government identifications cards, physical access credentials for automated building access control systems, as well as storage devices for logical access credentials. They will be issued to each Federal employee, contractor, and other affiliated individual as approved by Federal organizations for providing routine access to the defined facility. The Federal Smart Card Policy establishes the criteria for issuance, deployment, and management of smart cards within the Federal government, and should be consulted for further guidance.

The following basic expectations apply to smart card deployment:

- Identity data on the smart card must be in a standard machine-readable format
- Smart cards will be tamper resistant and counterfeit-resistant.
- Smart cards must support at least two-factor authentication for logical access.
- Smart cards must contain a FIPS-compliant cryptographic engine when used for cryptographic key generation and processing of encryption and digital signature requirements.
- Smart cards must allow post-issuance updating of data in a secure fashion
- Smart cards must allow for authentication of the token

8. Policy Implementation Requirements

This policy framework establishes the Common Policy implementation requirements for Federal Agencies, including the criteria intended to ensure uniform compliance with the Federal policy framework:

- Identity Credential Requirements: Agencies shall issue Federal Identity Credentials in a consistent manner, using approved identity proofing standards, and appropriate life cycle management practices. These credentials shall be the preferred method for seeking access to Federal facilities.

- **Physical Credential Requirement:** Agencies shall issue hardware tokens in a smart card form factor that is compliant with Government Smart Card Interoperability Specification (GSC-IS). These credentials will utilize a consistent topology to ensure government-wide recognition and will utilize a standard data format to ensure interoperability of electronic credentials and automated access systems.
- **Electronic Credential Requirement:** Agencies shall issue electronic authentication credentials to employees, contractors and other affiliate users of Federal systems, facilities and services. The electronic credentials shall be compliant with Federal standards and guidance, as represented in Federal policy documents.
- **Identity Assurance Requirements:** Agencies shall meet or exceed the minimum identity authentication requirements of this policy framework.
- **PKI Requirements:** Agencies that deploy PKI-based electronic authentication credentials must adopt the Common Federal PKI Certificate Policy, utilize Federal approved PKI Managed Service Providers, or participate in the Federal PKI through peer-to-peer cross-certification with the Federal Bridge CA, unless specifically exempted through the OMB budgetary process.
- The National Institute of Standards and Technology (NIST) shall issue and maintain standards and guidance required to support this policy framework.
- The Federal Identity Credentialing Committee shall determine common physical/logical access standards for the Federal government that support the intent of this policy framework, and are technically consistent with existing policies and procedures for identity assurance (e.g. EO 10450).

9. Shared Services Implementation Requirements

This policy framework requires that PKI managed service providers operating under the Common Federal PKI Certificate Policy are available for government-wide use in order for agencies to acquire and issue electronic credentials consistent with this policy. Such managed services will be offered under existing and new Federal contracts with PKI service providers, as modified to address the Common Federal PKI Certificate Policy.

10. Federal Identity Credentialing Component

The Federal Identity Credentialing Committee, thru its respective subcommittees, shall establish the business objectives, standards, and criteria for the Federal Identity Credentialing Component. This shall be communicated to the Component Subcommittee of the Architecture and Infrastructure Committee.

The Architecture and Infrastructure Committee, as chartered by the Federal CIO Council, is responsible for defining, assessing and managing common business and technology components. A standard Authentication infrastructure that supports all Federal identity management is considered a commonly used component and therefore will be managed in conjunction with the implementation and management processes defined and instituted by the CIO Council. These processes include:

- Determination of criteria for the selection of a commonly used component based on the Federal Identity Credentialing Committee inputs.
- Provision of a common repository for the identification and use of common components
- Definition of component use processes by agencies

The implementation of a standard Federal Identity Management component will be coordinated between the Federal Identity Credentialing Committee and the Architecture and Infrastructure Committee to ensure consistent, effective cross-agency use in concert with the requirements of this policy.