The Federal Identity, Credential, and Access Management Architecture

January 6, 2021

FINAL

Version 3.1

Identity, Credential, and Access Management Subcommittee (ICAMSC)

Table of Contents

Federal ICAM Architecture Introduction 2

Goals and Objectives 7

Services Framework 9

Use Cases 22

System Component Examples 46

Standards and Policies 50

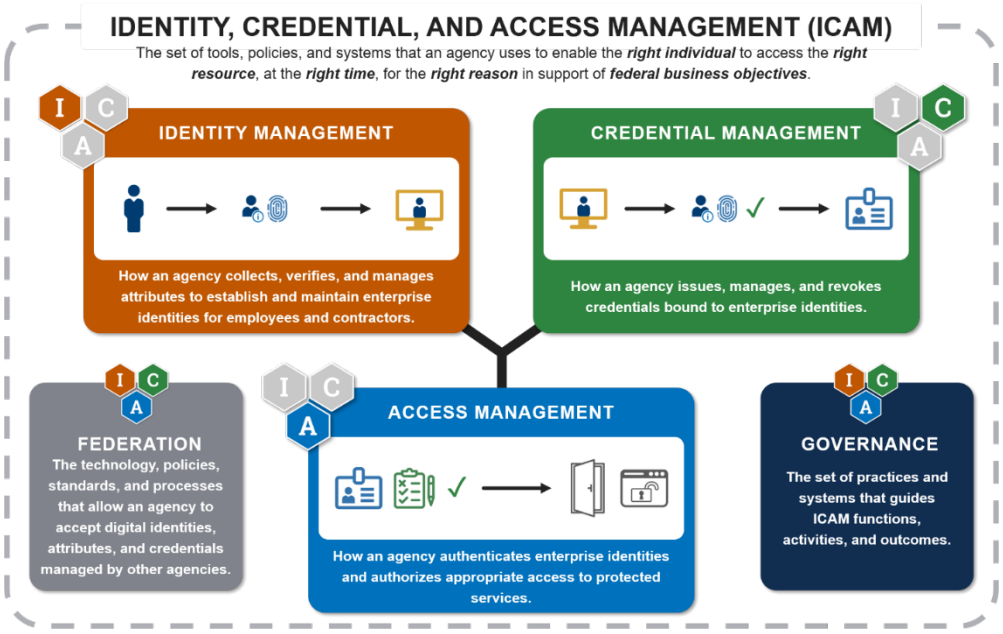
Federal ICAM Architecture Introduction

Federal Identity, Credential, and Access Management (FICAM) is the federal government's implementation of Identity, Credential, and Access Management (ICAM).

> ***ICAM*** is the set of tools, policies, and systems that an agency uses to enable the ***right individual*** to access the ***right resource***, at the ***right time***, for the ***right reason*** in support of ***federal business objectives***.

This version of the FICAM Architecture encompasses the **enterprise** ICAM policies, technologies, and system approaches for government employees, contractors, and authorized partners. Citizen interactions with the federal government - or consumer ICAM - are not covered under this version of the FICAM Architecture.

The following diagram is a high-level view of the ICAM practice areas and supporting elements.



The FICAM Architecture includes government-wide enterprise architecture views with the flexibility to support each agency's unique business or mission needs. Use the FICAM Architecture as a tool to continuously improve upon your agency's approach and align with federal security and privacy initiatives.

Copy the graphics and text throughout this playbook to use at your agency to drive ICAM awareness, strategy developments, and communications.

What Is ICAM?

ICAM is the set of tools, policies, and systems that an agency uses to enable the right individual to access the right resource, at the right time, for the right reason in support of federal business objectives.

Agencies implement ICAM services and solutions to unify their IT services, improve physical access control, and improve information security and decisions. Understanding the building blocks of ICAM is key to understanding the FICAM Architecture. ICAM has three practice areas and two supporting elements. The supporting elements enhance the capabilities of the practice areas.

ICAM Practice Areas	
	**Identity Management** is how an agency collects, verifies, and manages attributes to establish and maintain enterprise identities for employees and contractors.
	**Credential Management** is how an agency issues, manages, and revokes credentials bound to enterprise identities.
	**Access Management** is how an agency authenticates enterprise identities and authorizes appropriate access to protected services.
ICAM Supporting Elements	
	**Federation** is the technology, policies, standards, and processes that allow an agency to accept digital identities, attributes, and credentials managed by other agencies.
	**Governance** is the set of practices and systems that guides ICAM functions, activities, and outcomes.

What Is the FICAM Architecture?

FICAM is the federal government's enterprise approach to design, plan, and execute common ICAM processes.

The FICAM Architecture is a framework for an agency to use in ICAM program and solution roadmap planning. The FICAM Architecture focuses on enterprise identity processes, practices, policies, and information security disciplines.

> A federal enterprise identity is the unique representation of an employee, contractor, or enterprise user, which could be a mission or business partner, or even a device or technology managed by a Federal agency to achieve its mission and business goals (OMB Memorandum 19-17).

Who Is the FICAM Architecture for?

The FICAM Architecture is for agency personnel. An enterprise architecture is primarily used by:

- **Senior Federal IT and Agency Stakeholders** to understand the concepts for identity and access management services and the basic use cases supporting business objectives.
- **Program Managers** to find common definitions and frameworks for use in planning.
- **Enterprise and Application Architects** to use a common framework for designing and governing IT systems, applications, and implementations.

What Is the History of the FICAM Architecture?

The FICAM Architecture was created in 2009 to provide a common ICAM segment architecture for federal agencies. The FICAM Architecture was the primary foundation of what later became the *FICAM Roadmap and Implementation Plan* enhanced with complementary implementation sections.

In 2015, ICAM experts from across the federal government collaborated on an updated FICAM Architecture. This update was intended to be more concise, easy to understand,

and visually appealing while reflecting the latest updates in cybersecurity, enterprise architecture, and ICAM policy and technology.

This site contains the current 2020 update for the FICAM Architecture. The FICAM Roadmap and Implementation Guidance v2.0 is superseded by both the FICAM Architecture updates and other complementary modernized playbooks developed by ICAM committees across government.

Goals and Objectives

These Goals and Objectives identify the aims and outcomes of a federal agency enterprise ICAM program. The goals and objectives are for ICAM functions and map to government-wide policies, cross-agency priorities, and strategic government initiatives.

The goals are aspirational statements designed for senior government leaders, agency executives, and agency ICAM program leadership responsible for setting program strategy. The objectives are action areas where agency execution strategies, action plans, and performance metrics can be developed based on alignment with the mission needs.

The visual includes three goals, each with its own objectives.

Goal 1: Modernize security policies and solutions to make risk-based decisions, automate identity and access management processes, and move access protections closer to government data.

- 1.1 - Review, update, and maintain comprehensive ICAM policies and technology solution roadmaps to inform and enforce enterprise strategic planning, risk management, and modernization.
- 1.2 - Adopt and use cloud-ready systems that provide an efficient and secure way to access resources.
- 1.3 - Monitor and respond to user behavior and events by using data as a strategic asset to make adaptive and risk-based decisions.

Goal 2: Enable missions to efficiently deliver services to federal and contractor employees and resources.

- 2.1 - Establish and manage identities for all enterprise users and resources.
- 2.2 - Design enterprise solutions to manage access to information and resources.
- 2.3 - Utilize enterprise identity information discovery and enterprise centralized access management.
- 2.4 - Leverage federated solutions to accept identity and authentication assertions made by other agency and mission partners when efficient.

Goal 3: Provide enterprise-level solutions within agencies to improve operations and promote cost-effective and efficient use of resources.

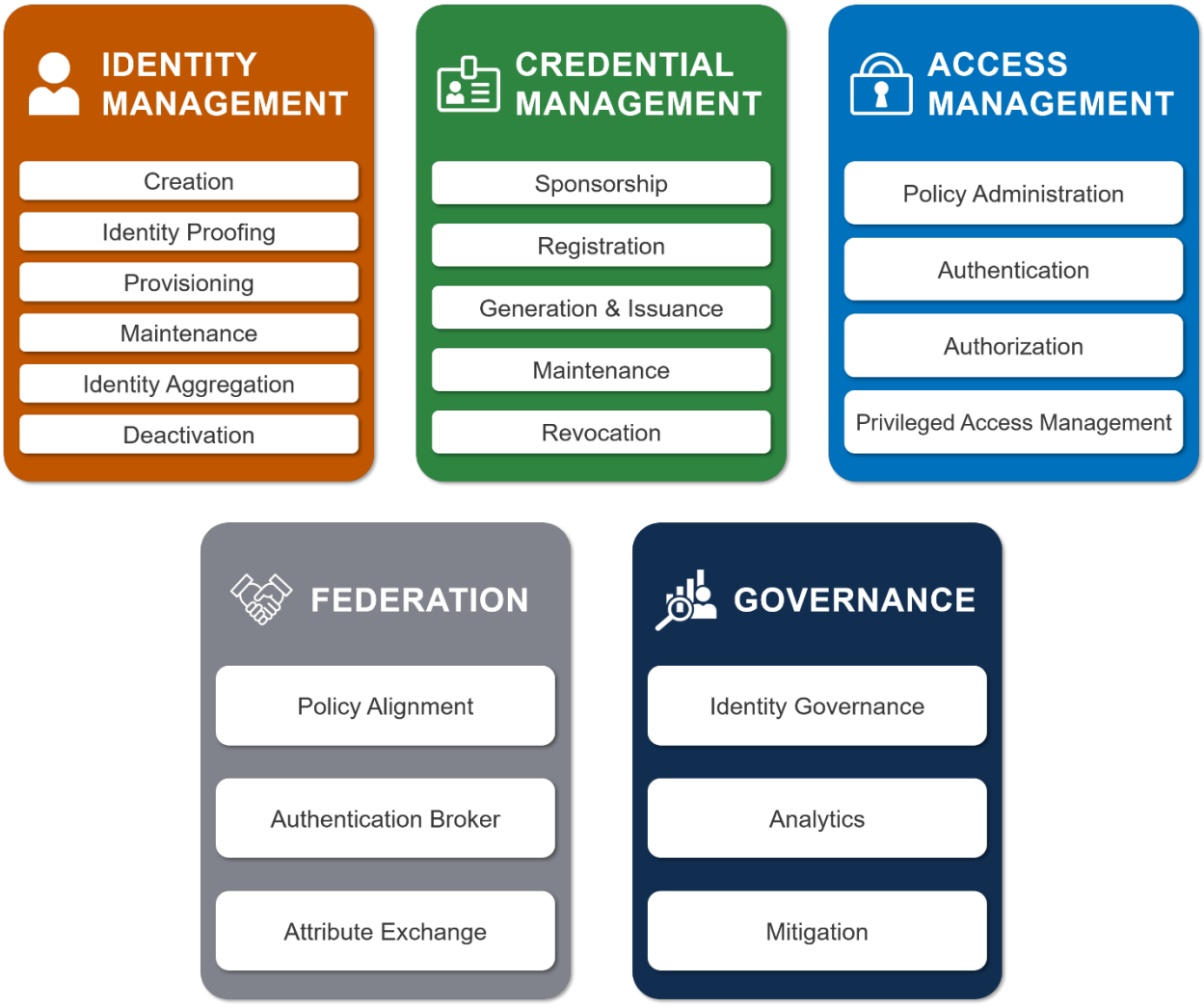
- 3.1 - Streamline ICAM governance and program management within each agency to optimize execution, ensure consistency, and align intent across the enterprise.
- 3.2 - Evaluate, rationalize, and migrate to modern, cloud-smart solutions for ICAM services.
- 3.3 - Promote interoperability and efficiency across the federal government by buying and building ICAM solutions that use open, commercially adopted standards.

Services Framework

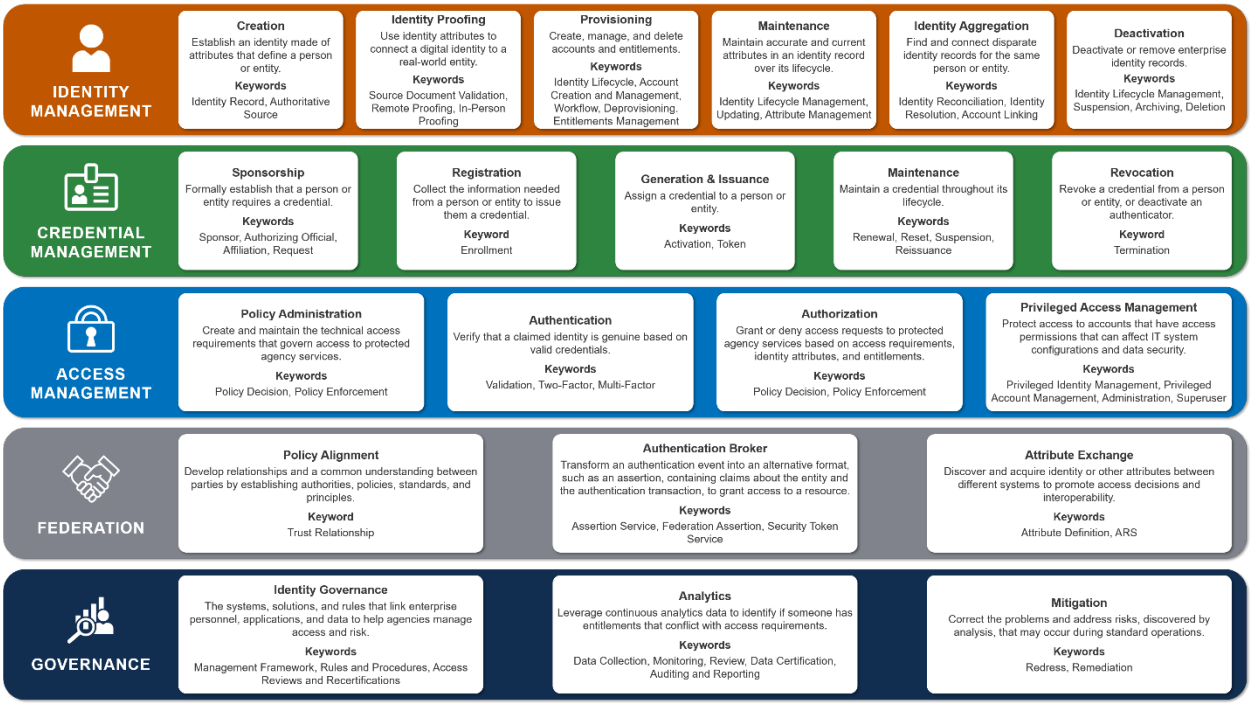
The Services Framework identifies the services that provide functionality within the scope of ICAM. The Services Framework is a tool for you to help translate between business requirements and technical solutions.

The Services Framework is designed for ICAM program managers and information technology enterprise architects.

FICAM Practice Areas

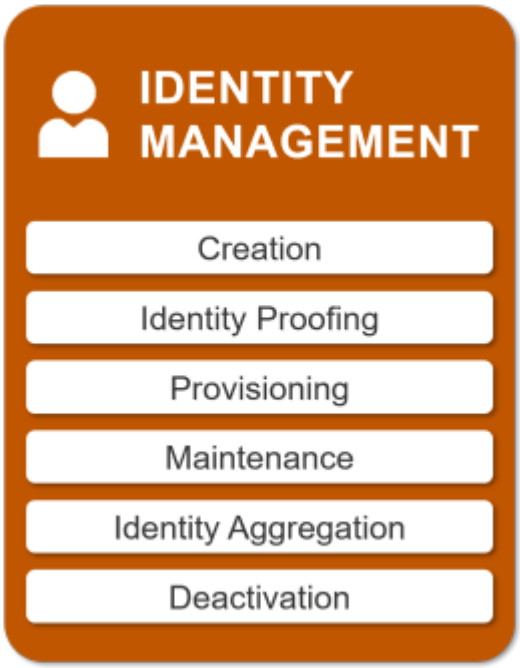


FICAM Services



Identity Management

Identity Management is how an agency collects, verifies, and manages attributes to establish and maintain enterprise identities for federal government employees, contractors, and authorized mission partners. This service does not apply to public or consumer identity management.



An enterprise identity record is the set of attributes, or characteristics, that describe a person within a given context:

- Your identity within your agency's Human Resources (HR) system is different from your personal identity at your bank.
- A person's identity as a government contractor is different from their identity as an Army Reservist.

Although your identity remains the same over time, it evolves as your attributes change, such as when you get a promotion, change your name, receive additional training, or retire.

Agencies should manage identity attributes as centrally as possible and distribute them as needed. The following are some examples of identity attributes:

- *Core identity attributes* - First name, last name, and address of record.
- *Contact attributes* - Physical location, government phone number, and government email address.
- *Authorization attributes* - Clearance, training, and job codes.

Identity proofing is how an agency verifies an enterprise identity. The complexity of this process depends on the Identity Assurance Level (IAL) you require for an identity. Federal agencies require a minimum IAL3 for employees and contractors. For example, a federal employee or contractor presents identity attributes via a driver's license or utility bill. The agency verifies the identity documents and the individual's photo (biometric).

An identifier is a unique attribute used to locate an identity in a system:

- While your agency may issue Personal Identification Verification (PIV) cards to multiple people named John Smith, each has a different PIV card number.
- While your agency may have more than one employee named Jane Smith, each employee has a unique email address tied only to their identity.

Identity Management Services

The Identity Management services in the Federal ICAM architecture include Creation, Identity Proofing, Provisioning, Maintenance, Identity Aggregation, and Deactivation. These services are sometimes collectively known as Identity Lifecycle Management.

Creation

Establish an identity made of attributes that define a person or entity.

Keywords: Identity Record, Authoritative Source

Identity Proofing

Use identity attributes to connect a digital identity to a real-world entity.

Keywords: Source Document Validation, Remote Proofing, In-Person Proofing

Provisioning

Create, manage, and delete accounts and entitlements.

Keywords: Identity Lifecycle Management, Workflow, Deprovisioning, Account Management, Account Creation, Entitlements Management

Maintenance

Maintain accurate and current attributes in an identity record over its lifecycle.

Keywords: Identity Lifecycle Management, Updating, Attribute Management

Identity Aggregation

Find and connect disparate identity records for the same person or entity.

Keywords: Identity Reconciliation, Identity Resolution, Account Linking

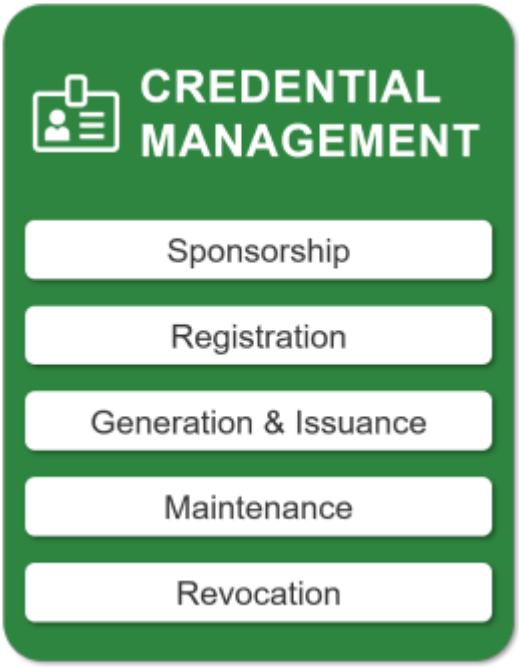
Deactivation

Deactivate or remove enterprise identity records.

Keywords: Identity Lifecycle Management, Suspension, Archiving, Deletion

Credential Management

Credential Management is how an agency issues, manages, and revokes credentials bound to enterprise identities.



A credential is a data structure that authoritatively binds an authenticator to an existing identity using one or more identifiers.

The following are types of authenticators:

- Something you know, like a password or PIN.
- Something you have, like a private key or One-Time Password (OTP) generator.
- Something you are, like a fingerprint or iris.

The Authenticator Assurance Level (AAL) determines the authenticators associated with a credential. Federal government-wide policy requires a minimum Authenticator Assurance Level 2 for employees and contractors.

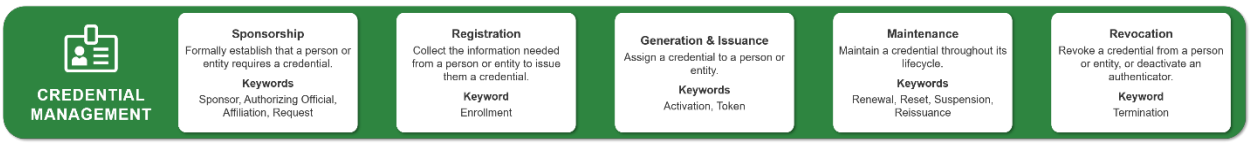
The following are some examples of credentials:

- You might use an agency-issued smart card, such as a PIV or CAC, that includes a picture and cryptographic key pairs to assert your identity at a federal facility.
- You might use a combination of credentials, like a username/password with an OTP generated by a mobile application, to assert your identity to a federal web application.

Unlike identities, credentials can expire. If an enterprise identity continues past a credential's expiration date, the issuing agency can issue a new credential.

Credential Management Services

The Credential Management services in the FICAM architecture include Sponsorship, Registration, Generation & Issuance, Maintenance, and Revocation.



Sponsorship

Formally establish that a person or entity requires a credential.

Keywords: Sponsor, Authorizing Official, Affiliation, Request

Registration

Collect the information needed from a person or entity to issue them a credential.

Keyword: Enrollment

Generation & Issuance

Assign a credential to a person or entity.

Keywords: Activation, Token, Authenticator

Maintenance

Maintain a credential throughout its lifecycle.

Keywords: Renewal, Reset, Suspension, Reissuance

Revocation

Revoke a credential from a person or entity, or deactivate an authenticator.

Keyword: Termination

Access Management

Access Management is how an agency authenticates enterprise identities and authorizes appropriate access to protected services.

Policy administration is a combination of laws, regulations, rules, and agency policies that secure access to agency services. Your agency determines the requirements for an individual to access each resource category, and they can be as simple or as complex as you need. The following are some examples of access requirements:

- "Grant access to anyone on this list of people."
- "Grant access to any agency employee or contractor with an authenticated PIV card."
- "Grant access to anyone who is a federal employee, GS-12 or higher, cleared Top Secret, trained in first aid, and certified as a project manager."

Authentication

Authentication is how you verify the claimed identity of someone trying to access an agency resource. Typically, you'll verify an identity using an authenticator associated with a credential.

Authentication is generally a two-step process:

Step 1. Authenticate the credential itself:

- Did a trusted organization issue the credential?
- Has the credential expired?
- Has the credential been revoked, voided, or tampered?

Step 2. Ensure the individual that the credential was issued to is the same individual that is presenting it:

- Do the photo and attributes on the credential match the person who presented it?
- Does the person know the PIN for the credential?
- Does the person have the private key on the smart card for the certificate presented to a website?

Authorization

Authorization is how you decide whether you should allow someone to access an agency resource. Access requirements usually dictate whether you'll allow someone to:

- Read or modify a certain document.
- Access an agency website.
- Enter an agency facility or location.

Usually, authorization occurs immediately after authentication. When you log in to a service, you present your credentials and the service confirms your credentials are valid (authentication) and grants or denies you access based on your assigned permissions (authorization).

Authorizations are based on four models:

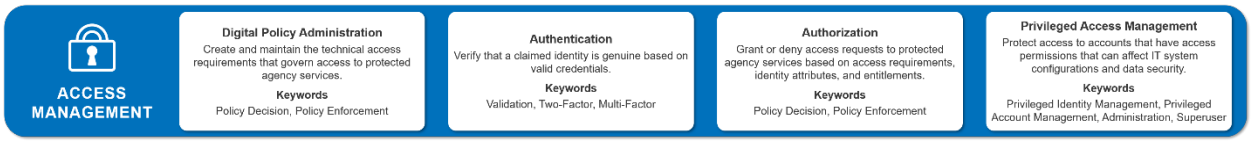
- Access Control Lists (ACLs)
- Role-Based Access Control (RBAC)
- Policy-Based Access Control (PBAC)
- Attribute-Based Access Control (ABAC)

Each of these authorization models has benefits and limitations. The policies and access requirements defined by agency business owners help inform the model used to best suit their needs. More robust access control models, such as ABAC, can help agencies with improved automation and are increasingly adopted by cloud-native and cloud-friendly services.

Identity proofing is how you establish an identity. Authentication is how you confirm the identity. Authorization is how you use the identity.

Access Management Services

The Access Management services in the federal ICAM architecture include Policy Administration, Entitlements Management, Authentication, Authorization, and Privileged Access Management.



Digital Policy Administration

Create and maintain the technical access requirements that govern access to protected agency services.

Keywords: Policy Decision, Policy Enforcement

Authentication

Verify that a claimed identity is genuine based on valid credentials.

Keywords: Validation, Two-Factor, Multi-Factor

Authorization

Grant or deny access requests to protected agency services based on access requirements, identity attributes, and entitlements.

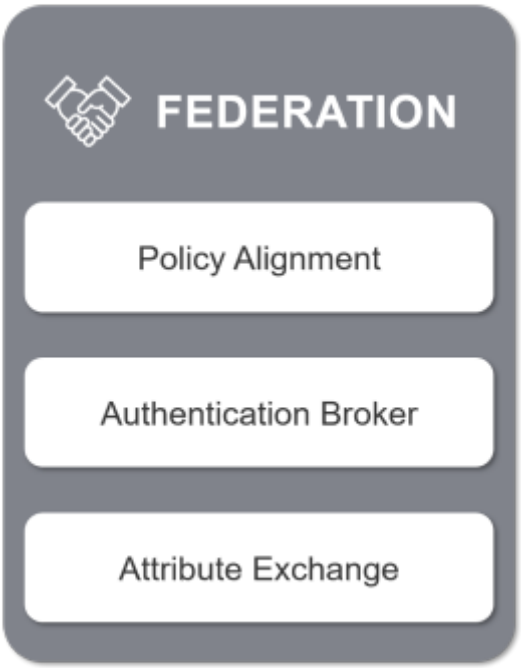
Keywords: Policy Decision, Policy Enforcement

Privileged Access Management

Protect access to accounts that have access permissions that can affect IT system configurations and data security (e.g., superusers, domain administrators, or global administrators).

Keywords: Privileged Identity Management, Privileged Account Management, Administration, Superuser

Federation



Federation is the technology, policies, standards, and processes that allow an agency to accept digital identities, attributes, and credentials managed by other agencies.

Federation has many different applications, including:

- *Accepting an authentication transaction from another organization:*

Agency A authenticates one of its users and passes identity attributes and transaction details to Agency B. Agency B grants access to an application for that identity.

- *Accepting specific characteristics (i.e., attributes such as identifiers) describing an individual from another organization:*

An individual can use their agency-issued credential containing an internal identifier(s) to directly log in to a different agency's online service. The online service registers the identifier(s) in their system for future use.

Federation Services

The Federation services in the FICAM architecture include Policy Alignment, Authentication Broker, and Attribute Exchange.

Policy Alignment

Develop relationships and a common understanding between parties by establishing authorities, policies, standards, and principles.

Keyword: Trust Relationship

Authentication Broker

Transform an authentication event into an alternative format, such as an assertion, containing claims about the entity and the authentication transaction, to grant access to a resource.

Keywords: Assertion Service, Federation Assertion, Security Token Service

Attribute Exchange

Discover and acquire identity or other attributes between different systems to promote access decisions and interoperability.

Keyword: Attribute Definition

Governance

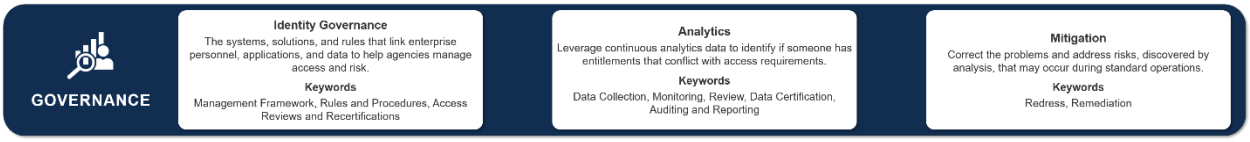
Governance is the set of practices and systems that guides ICAM functions, activities, and outcomes.

To perform effective governance, agencies must collect data about ICAM functions from many sources, such as policies and entitlements stores, and analyze this data. Proper data analytics help agencies monitor compliance with established information security policies.

If your agency identifies problems during data collection and analysis, you should remediate these issues as quickly as possible. Real-time monitoring and risk mitigation is crucial to ensure employees and contractors have only the appropriate access, following the principle of least privilege.

Governance Services

The Governance services in the FICAM architecture include Identity Governance, Analytics, and Mitigation.



Identity Governance

The systems, solutions, and rules that link enterprise personnel, applications, and data to help agencies manage access and risk.

Keywords: Management Framework, Rules and Procedures, Access Reviews and Recertifications

Analytics

Leverage continuous analytics data to identify if someone has entitlements that conflict with access requirements.

Keywords: Data collection, Monitoring, Review, Data Certification, Auditing and Reporting

Mitigation

Correct the problems and address risks, discovered by analysis, that may occur during standard operations.

Keywords: Redress, Remediation

Use Cases

These use cases are designed for ICAM Enterprise Architects and business owners and describe some of the most common ICAM business processes.

Each use case includes a high-level summary of the scenario, individuals and systems involved in the use case, illustrations that show the required steps to achieve the end goal, and an icon that indicates the practice area and the service with which the use case most closely aligns.

For details about ICAM services, see the Services Framework.

While each use case describes a particular ICAM business process, the use cases are all interrelated. The use cases generalize the activities and technologies to make sure they apply across many agencies. The use cases don't include agency-specific functions and process details because your agency should analyze your systems and processes to align with these broad use cases.

You can combine or build upon the ICAM use cases to support your agency's scenarios and needs.

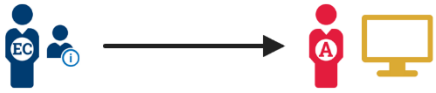
1. Create and Maintain an Identity

When you onboard an employee or contractor at your agency, you collect identity information from the individual and store parts of that information as identity attributes. These attributes serve as a digital proxy for the individual's identity, also known as an enterprise identity.

Use Case

In this use case, an administrator needs to collect or manage identity data for an employee or contractor for the purpose of creating an enterprise identity record and maintaining it throughout its lifecycle.

1. Collect information



The administrator collects identity information from the employee or contractor.

This identity information may come from the individual, onboarding documents, or HR systems.

2. Create an enterprise identity

The administrator adds the identity information to the authoritative source, a data repository.

Result: An enterprise identity in the authoritative source for the employee or contractor.

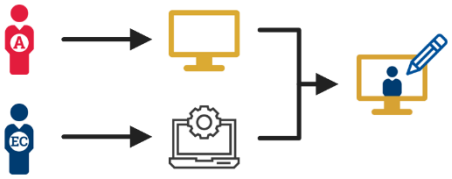
3. Maintain the enterprise identity

The following steps describe identity maintenance your agency should perform on a regular basis.

3a. Identify and aggregate identity data

Query your data repositories for any existing identities for an individual. Aggregate these attributes as a single enterprise identity for the individual.

3b. Update the enterprise identity



If an individual has updated personal information, there are two ways to update the enterprise identity:

- The administrator updates the individual's enterprise identity attributes directly in the authoritative sources.
- The individual uses an agency application to update their personal information, and the application updates the individual's enterprise identity attributes in the authoritative sources.

3c. Delete the enterprise identity

When you need to delete an enterprise identity, delete the identity attributes in the authoritative source.

Example

I want to create a new enterprise identity so that an individual may be established as a federal employee or contractor that will need to be identity proofed, credentialed, and granted access to agency services.

2. Proof an Identity

Before you can create a credential and assign it to an individual, that person must provide proof of their claimed identity. Identity proofing is the process by which a federal agency collects and verifies information about a person to establish an enterprise identity.

The location or information that a person needs to access informs the Identity Assurance Level (IAL), which determines the elements you should require from that person for identity proofing. There are three IALs; however, federal agencies require a minimum of IAL2 for employees or contractors with recurring access to government resources, so these use cases do not include IAL1.

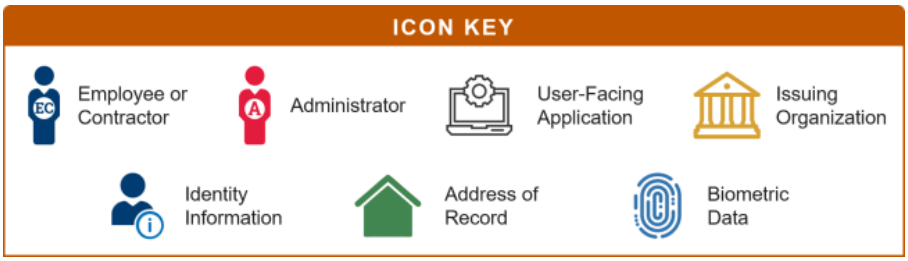
This use case describes the high-level steps to proof an identity at IAL2 or IAL3. Depending on the required IAL, you may require increasingly more information from an employee or contractor or partner along with additional verification steps. The information provided by the employee or contractor is also known as identity evidence. Identity evidence may be physical, such as passports, driver's licenses, and birth certificates.

- **IAL2** - first and last name, email address, and address of record, supported by appropriate identity documentation and verified as strong.
- **IAL3** - first and last name, email address, address of record, and fingerprints, supported by appropriate identity documentation and verified as superior.

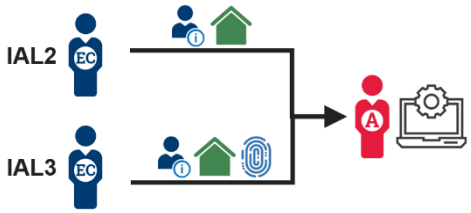
For more information about identity proofing and IALs, see NIST SP 800-63-A (Section 2.2).

Use Case

In this use case, an administrator needs to collect or manage identity data for an employee or contractor for the purpose of creating an enterprise identity record and maintaining it throughout its lifecycle.



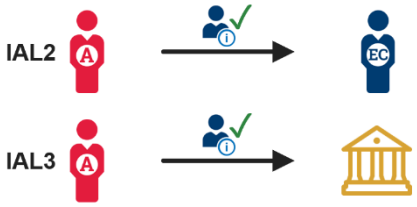
1. Collect identity information



IAL2 *(In-person or remote)* - The employee or contractor presents identity information, like first name, last name, and address of record.

IAL3 *(In-person or supervised remote)* - The employee or contractor presents identity information, like first name, last name, and address of record, and biometric data like fingerprints.

2. Verify the identity information



IAL2 - The administrator confirms the information provided is valid and current by comparing photo identification to the individual, or confirming contact information, ensuring it matches the provided documentation.

IAL3 - The administrator verifies all information with the issuing organization.
Result: The individual's identity has been successfully proofed at IAL2, or IAL3.

Examples

- I want to proof the identity of an employee or contractor to verify that the individual is who she says she is so that she can be issued a unique enterprise credential.
- A prospective employee or contractor has filled out their information in an HR system and requires IAL3 proofing and minimum background investigations. The prospective employee/contractor is then scheduled for in-person proofing. The prospective employee/contractor brings required identity documentation; the information is verified using approved documentation and biometrics are captured.

3. Manage the Entitlements Lifecycle

You can assign access entitlements to individuals, roles, and groups. These entitlements define an employee or contractor's access to agency services, so you'll need to assign entitlements before an employee or contractor can access an agency service.

Use Case

In this use case, an administrator needs to assign entitlements to an employee or contractor.

1. Initiate the request

An individual requests entitlements, or joins a team with specific access requirements.

The requestor may be the employee or contractor, their supervisor, HR, or a security team member.

2. Review the request

The administrator compares the employee or contractor's requested entitlements with the relevant access requirements.

If the employee or contractor qualifies for the requested entitlements and has a mission need for access, the administrator approves the request.

3. Assign the entitlements

The administrator assigns the entitlements to the employee or contractor.

Any time the employee or contractor's role or relationship changes, the administrator updates the entitlements accordingly, including removing entitlements as needed.

Examples

- I want to indicate that an employee or contractor requires and is allowed access to an agency service so that they can access the service when needed.
- An employee is hired to be part of the financial review team and requires access to financial applications. The employee has a role assigned to their enterprise identity record and associated with their identity attributes.

4. Create and Issue a Credential

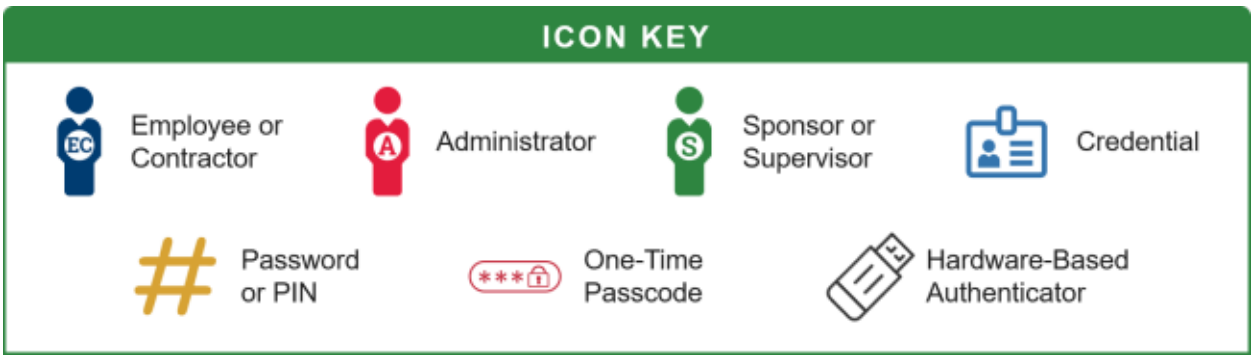
After you identity proof an individual, you'll issue some proof of that individual's claimed identity. A credential (like a physical card) is a type of authenticator that serves as a tool for an employee or contractor to gain access to agency services.

Use Case

In this use case, an administrator needs to issue a credential to an employee or contractor.

Note: The preferred credential for employees and contractors is a PIV card. For cases where you cannot issue a PIV card, you must use a combination of factors to reach at least an Authenticator Assurance Level 2 (AAL2) credential.

For more information about authentication and AALs, see NIST SP 800-63-B (Section 4).



1. Initiate the request

An individual presents a valid government issued ID.

2. Review the request

The government ID is verified with the organization that issued it.

3. Generate and assign the authenticator(s)

Generate and assign the authenticator to the individual.

Example

I want to issue an enterprise credential, unique to an employee or contractor, so that they are able to access federal buildings and protected resources to which they require access.

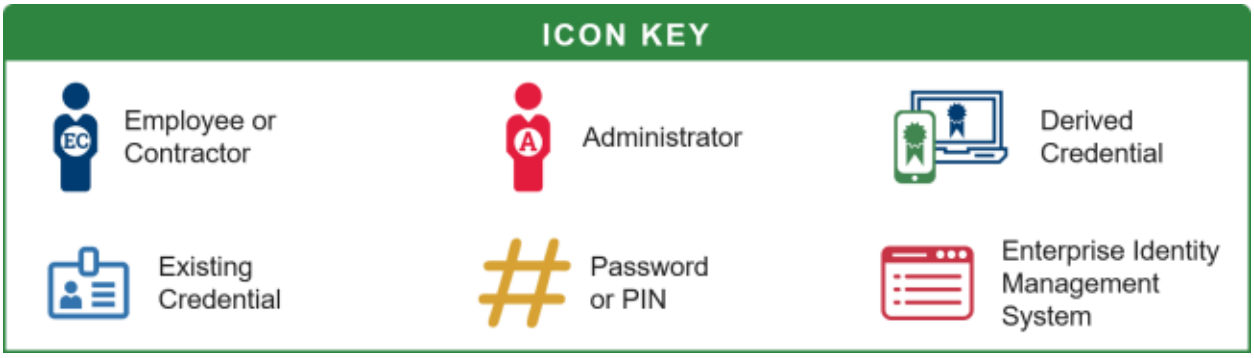
5. Issue a Derived Credential

A derived credential is a credential derived from an existing credential, with a different form factor, such as a credential on a mobile device. Derived credentials have the same IAL as the existing credential and the same or lower AAL.

When an employee or contractor requires authentication but cannot leverage an existing credential, they can use a derived credential. To be eligible for a derived credential, the employee or contractor must already have a valid credential with Authenticator Assurance Level (AAL) 2 or 3.

Use Case

In this use case, an employee or contractor interacts with the agency services to register or request a derived credential.



1. Initiate the request

A request for identity data is initiated to the identity manager.

This identity manager could be a person or system, depending on the organization.

2. Authenticate the existing credential

The identity manager identifies relevant sources of data on the individual.

Sources could include HR systems, security data, and personal databases.

3. Generate the derived credential

Generate the derived authenticator and note the change in the user's enterprise identity record.

Examples

- I want to provide an employee or contractor, who has already been issued an enterprise credential, a derived credential so that they can authenticate to enterprise applications.
- An employee or contractor travels quite a bit as part of their job. Accordingly, they are frequently limited to using a small tablet or their phone to stay connected while on the go. In this case, a derived credential is needed for purposes such as accessing secure agency websites or an agency VPN from their mobile device.

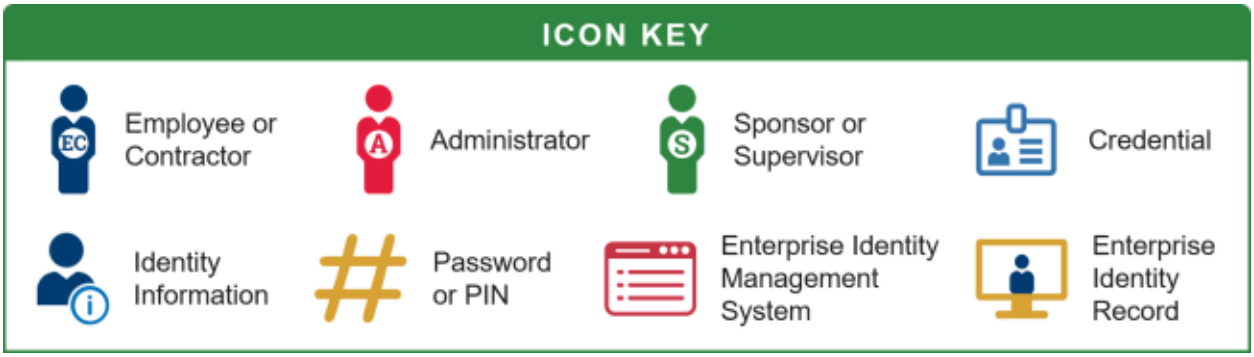
6. Manage the Credential Lifecycle

Active credentials require regular maintenance. This use case describes the most common credential maintenance activities:

- **Reset a credential** - An employee or contractor forgets the password or PIN associated with a credential and requests a reset.
- **Renew a credential** - An employee or contractor's credential is expiring or their identity information changes, so they request a replacement credential. You must renew a credential prior to the expiration date; otherwise, the employee or contractor must go through the issuance process again.
- **Revoke a credential** - An employee or contractor is no longer eligible for their credential (like separating from the issuing agency). The sponsor, supervisor, or administrator requests a revocation of all associated credentials and enterprise accounts.

You should periodically review your employee or contractors' eligibility for credentials to identify potential orphaned data.

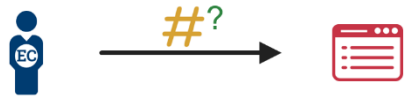
Use Cases



Reset a Credential

In this use case, an administrator needs to reset a password or PIN for an employee or contractor credential.

1. Initiate the request



An employee or contractor forgets their password or PIN, and requests a reset.

If the request is valid, the identity management system approves the request.

2. Issue a reset

The system issues a password/PIN reset, which may be a temporary password or a link to a web-based reset form.

3. Reset the credential

The employee or contractor resets their password or PIN.

Renew a Credential

In this use case, an administrator needs to issue a new credential to replace one that will expire soon or has outdated identity information.

1. Initiate the request

An individual requests a renewal for an employee or contractor's credential.

This individual may be the employee or contractor, their supervisor, or an administrator with approval authority.

This could also be an automated process triggered by schedules or specific events.

2. Review the request

The identity management system reviews the request and verifies that the employee or contractor qualifies for a renewed credential. If so, approve the request.

3. Replace the credential

The system issues a new credential to the employee or contractor, and updates the associated enterprise identity record.

Revoke a Credential

In this use case, an administrator needs to revoke an active credential.

1. Initiate the request

An individual sends a separation notification or a notice of a lost or compromised credential, requesting revocation.

This individual may be the employee or contractor, their supervisor, HR, or a security team member.

2. Disable the credential

The administrator invalidates the credential.

Depending on your agency, an individual or a system may perform this task.

3. Return the credential

If the revoked credential is physical or hardware-based, the administrator returns the credential to the appropriate individual.

This individual may be a supervisor, HR, or security team member.

Examples

- An employee or contractor may have attempted to use a credential and input the PIN information incorrectly several times up to an agency-defined limit and has locked their account or credential. The employee or contractor requests a PIN reset. The employee or contractor is directed to an unlock service; has to verify information again to prove they are the same person issued the original credential; and follows prompts to unlock their credential, generating a new PIN in the process.
- *Reset* - I want to verify the identity of an employee or contractor that has already been issued a credential and reset their PIN or password so that they can continue to access enterprise resources.
- *Renew* - I want to verify the identity and eligibility of an employee or contractor, who has a previously issued credential that is near expiration, so that they may be issued a new enterprise credential to maintain their ability to access enterprise resources.

- *Revoke* - I want to remove access to enterprise resources for an employee or contractor so that they can no longer use the protected resource.

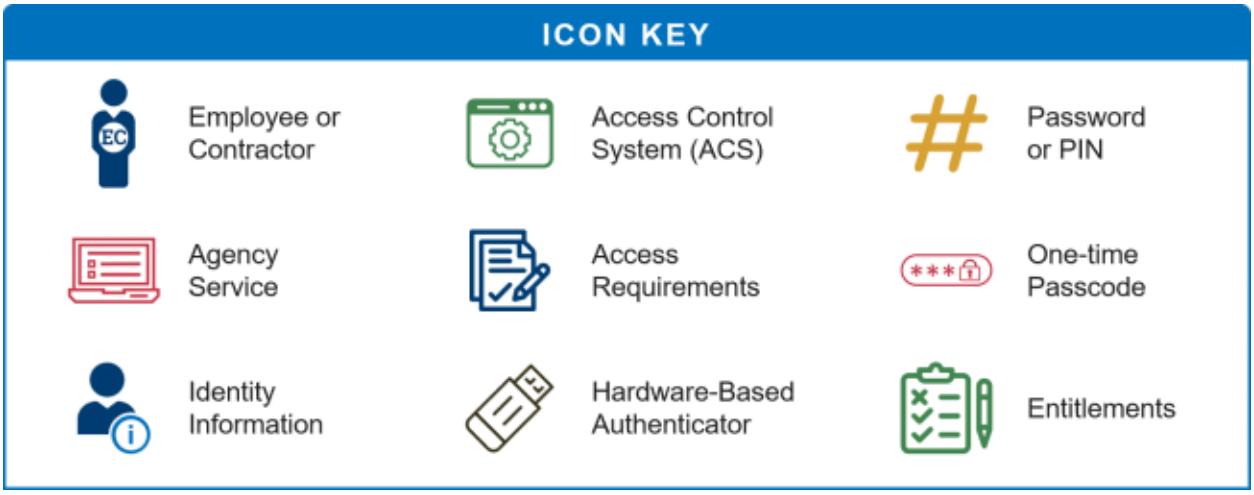
7. Grant Access

This use case describes the steps to authenticate individuals and authorize access to agency services. Agency services can be anything from applications and files to physical facilities.

Use Case

In this use case, an Access Control System (ACS) Administrator needs to grant access to an employee or contractor who has an enterprise identity and active credential and needs to access a logical or physical resource. These steps assume the employee or contractor already has credentials to support authentication as well as the access entitlements to support authorization decisions.

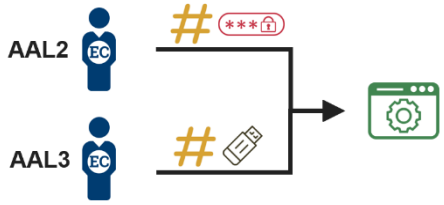
- *Authentication* - I want to verify the claimed unique identity of a given employee or contractor so that the system can verify the right individual is attempting to access an agency service.
- *Authorization* - I want to allow access for only employees and contractors that meet established requirements so that only the people who should have access do have access.



1. Access Attempt

An employee or contractor attempts to access an agency service.

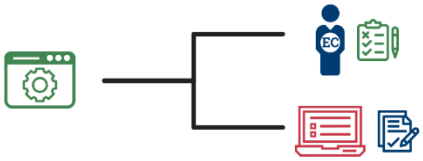
2. Authenticate the employee or contractor



The employee or contractor presents an authenticator to the ACS that meets the protected resource's minimum assurance requirements:

- **AAL2** (two-factor) - Something you know + something you have, like a one-time passcode.
- **AAL3** (two-factor + hardware) - Something you know + something you have, like a one-time passcode generated by a hardware-based authenticator; or a PIV credential. For more information about AAL values, see NIST SP 800-63B, Section 5: Authenticator and Verifier Requirements.

3. Determine the access entitlements and access requirements



Upon successful authentication, the ACS identifies 1) The employee or contractor's access entitlements associated with the protected resource, and 2) The protected resource's access requirements.

4. Process the access information

The ACS compares the employee or contractor's access entitlements to the protected resource's access requirements to decide whether to authorize access.

5. Grant access

If the employee or contractor meets the protected resource's access requirements, the ACS grants access to the protected resource.

The ACS logs the access attempt and decision for auditing purposes.

Example

An employee on the financial review team attempts to access a government financial application that is secured by a single sign-on (SSO) solution. The employee clicks a link to the financial application and is redirected to the SSO portal. The employee authenticates using his/her provided credential, which the SSO determines to be valid. The SSO solution or the financial application system finds the employee's enterprise identity account and compares the roles assigned to those allowed by the financial application. The resulting determination is that the employee has authenticated to the required assurance level and has the appropriate entitlements to access the system and is subsequently logged on.

8. Accept Federation Assertions

Federal employees and contractors often need to access protected services managed by other federal agencies. Federation is the means by which an agency can accept authentication assertions and associated identity attributes from systems within their agency and at other agencies. This allows federal employees and contractors from across agencies to access protected resources and streamlines the user's experience.

Agencies can pass assertions to share attributes about employees and contractors.

Use Case

In this use case, an employee or contractor from Agency A attempts to access a federated service at Agency B. This use case assumes the employee or contractor already has an account or entitlements to access resources at Agency B, or that they will be provisioned.

For more information about granting access to protected resources, see Grant Access.

1. Request access to federated service

An Agency A employee or contractor requests access to a federated service at Agency B.

The employee or contractor selects the Agency A authentication service.

2. Redirect to Agency A for authentication

The Agency B system redirects the employee or contractor to the Agency A authentication service.

Agency A authenticates the employee or contractor.

3. Perform transparent transaction

Agency A passes identity attributes and transaction data to Agency B via a signed assertion.

4. Agency B grants access

Agency B consumes the assertion data, optionally correlating it with an established account or local identity and makes an access control decision.

The Agency B system redirects the employee or contractor to the federated service.

Examples

- I want to allow other federal agencies' employees and contractors (who meet specific requirements) to access some of my agency's resources, which facilitates cross-government collaboration and information sharing.
- An employee or contractor from Agency A visits a shared service operated by Agency B to service all federal government users. At the homepage, the employee/contractor selects their Agency A icon and is redirected to their Agency

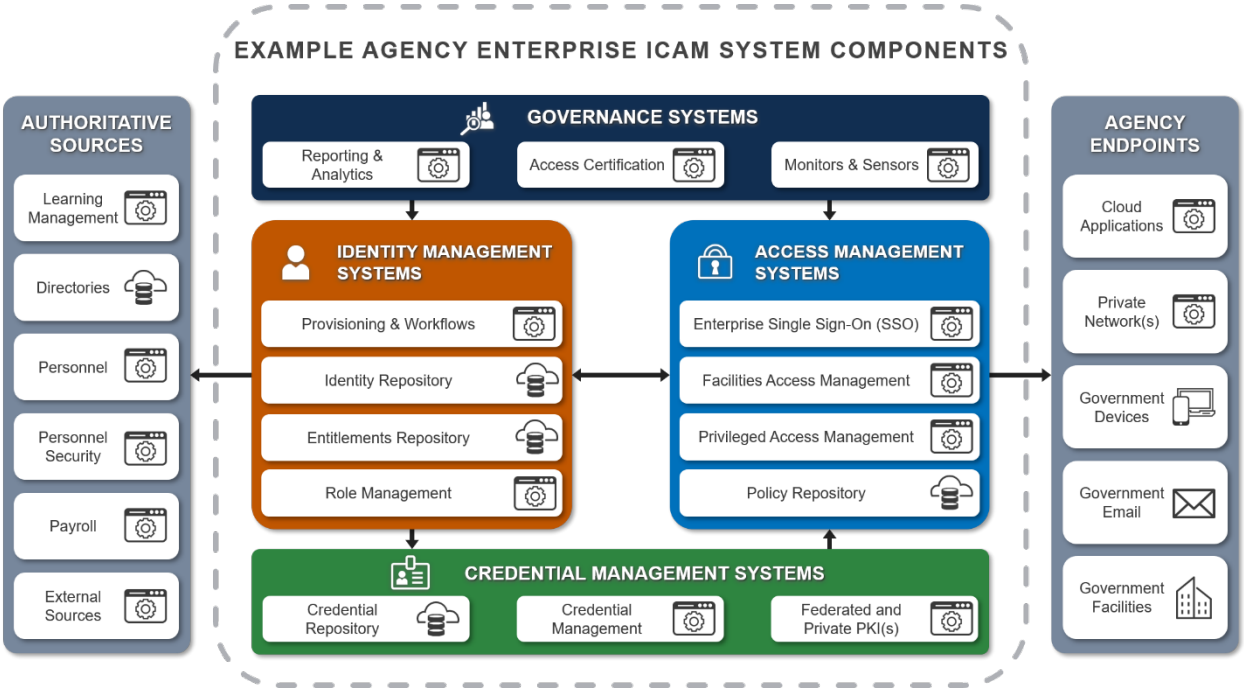
A SSO portal. They log in using their Agency A managed credentials and are redirected back to the Agency B shared service.

System Component Examples

Component examples include sample enterprise ICAM tools (e.g., solutions, applications, and software) aligned with ICAM service areas that illustrate ICAM functionality at an agency. The component examples are designed for enterprise architects, security engineers, and solution architects to facilitate discussions regarding the technology solutions to integrate with enterprise applications and the business requirements.

The systems components are representative examples only. Some solutions chosen by your agency may span across more than one service area.

The following figure is an example for a small selection of system components only. You can modify the graphic or incorporate it as is and target state system components for enterprise roadmap planning.



Authoritative Sources

An authoritative source is a trusted repository of identity attribute data. It's possible to have multiple authoritative sources for attributes.

Authoritative sources systems components may include:

- Human Resource systems such as payroll, time and attendance, and benefits administration
- Agency or government-wide Learning Management Systems
- Agency or government-wide Personnel Security systems for security and suitability
- Directory services, including on-premise or cloud-based directory services
- Other external or internal sources

Identity Management Systems

Identity management systems are how an agency manages the identity lifecycle.

Identity management system components may include:

- Identity lifecycle management services, including provisioning and workflow
- Role management or role manager applications
- Identity correlation or aggregation
- Directory management

Access Management Systems

Access management systems are how an agency leverages credentials to authenticate individuals and authorize access to protected resources.

Access management system components may include:

- Enterprise single sign-on (eSSO) applications
- Web access management applications
- Physical or facility access control systems
- Privileged access management applications
- Access policy and access rules repositories
- Policy enforcement points
- Policy decision points
- Virtual private networks
- Cloud access security brokers

- Network access management tools

Credential Management Systems

Credential management systems are how an agency manages an authentication token bound to an identity.

Credential management system components may include:

- PIV credential service provider solutions
- Other non-PKI credential service provider solutions
- Federated certification authorities
- Private certification authorities
- Key management services
- Enterprise certificate manager
- Multi-factor authentication managers for software and hardware tokens
- Password managers

Governance Systems

Governance is the set of components to centralize management, develop insights, and assist in managing ICAM areas and services. Applications across all service areas include auditing such as standard audit logs or configuration of auditable events. Governance includes the aggregation of individual auditing and reporting into centralized tools to perform real-time or near real-time analysis, identify anomalies, and trigger mitigations for anomalous authentication or authorization events. Tools are increasingly incorporating machine learning or adaptive algorithms.

Governance systems components may include:

- Identity governance solutions to perform access re-certifications
- IT Service Management (ITSM)
- Security information and event monitoring (SIEM)

Agency Endpoints

Agency endpoints are resources that an agency needs to protect, including physical and digital resources.

Agency endpoints may include:

- On-premise applications
- Cloud-based applications and platforms
- Agency private networks
- Government cloud email services
- Government facilities

Standards and Policies

Review the federal policies and standards that impact and shape the implementations of ICAM programs and systems.

Each section of this page lists documents in reverse chronological order, with the most recent documents first.

Laws

The Privacy Act of 1974 (September 2015)

> This Act protects certain federal government records pertaining to individuals. In particular, the Act covers systems of records that an agency maintains and retrieves by an individual's name or other personal identifier, such as a Social Security Number.

Federal Information Security Modernization Act (FISMA) of 2014 (December 2014)

> This Act provides a framework for measuring the effectiveness of federal information systems, and it calls for the development and implementation of continuous monitoring oversight mechanisms. It also acknowledges federal agencies should take advantage of commercially available security products (including software, hardware, etc.) that often provide robust information security solutions.

E-Government Act of 2002 (December 2002)

> This Act enhances the management and promotion of electronic federal services and processes by establishing a Federal CIO within the Office of Management and Budget (OMB) and by establishing a broad framework of measures that require using Internet-based information technology (IT) to enhance citizen access to government information and services and for other purposes.

Electronic Signatures in Global and National (ESIGN) Commerce Act of 2000 (June 2000)

This Act facilitates the use of electronic records and electronic signatures in interstate and foreign commerce by ensuring the validity and legal effect of electronic contracts.

Government Paperwork Elimination Act of 1998 (GPEA) (October 1998)

This Act requires federal agencies to allow individuals or entities that deal with the agencies the option to submit information or transact with the agency electronically when possible and to maintain records electronically when possible. This Act specifically states that electronic records and their related electronic signatures cannot be denied legal effect, validity, or enforceability just because they are in electronic form. This Act also encourages federal government use of a range of electronic signature alternatives.

Policies

Office of Personnel Management Memorandum: Temporary Procedures for Personnel Vetting and Appointment of New Employees during Maximum Telework Period due to Coronavirus COVID-19 (March 2020)

Temporary. This memorandum sets forth *temporary procedures* for the vetting and appointment of federal personnel, collection of biometrics for federal employment, and employment authorization and eligibility.

M 20-19: Harnessing Technology to Support Mission Continuity (PDF, March 2020)

Temporary. This memorandum directs that agencies utilize technology to the greatest extent practicable to support mission continuity during the national emergency. By aggressively embracing technology to support business processes, the federal government is better positioned to maintain the safety and well-being of the federal workforce and the American public while supporting the continued delivery of vital mission services. The set of *frequently asked questions* are intended to provide additional guidance and further assist the IT workforce as it addresses impacts.

M-19-17: Enabling Mission Delivery through Improved Identity, Credential, and Access Management (ICAM) (PDF, May 2019)

> This memorandum sets forth the federal government's ICAM policy. To ensure secure and efficient operations, agencies of the federal government must be able to identify, credential, monitor, and manage subjects that access federal resources. This includes information, information systems, facilities, and secured areas across their respective enterprises. In particular, how agencies conduct identity proofing, establish enterprise digital identities, and adopt sound processes for authentication and access control significantly affects the security and delivery of their services as well as individuals' privacy.

M-19-03: Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset (HVA) Program (PDF, December 2018)

> With the creation of the HVA initiative in 2015, the federal government's CFO Act agencies took a pivotal step toward the identification of its most critical assets. DHS, in coordination with OMB, established a capability to assess agency HVAs, resulting in the identification of critical areas of weakness and plans to remediate those areas of weakness. It established three possible categories for designating federal information or a federal information system as an HVA: Informational Value, Mission Essential, or Federal Civilian Enterprise Essential (FCEE). It also updates the required approach for agencies to report, assess, and remediate HVAs to protect against cyberattacks.

Executive Order 13833: Enhancing the Effectiveness of Agency Chief Information Officers (CIOs) (May 2018)

> This executive order authorizes federal agency CIOs to ensure that agency IT systems are as modern, secure, and well-managed as possible to reduce costs, mitigate cybersecurity risks, and deliver improved services to the American people.

Executive Order 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (May 2017)

This executive order places an emphasis on modernizing and securing federal networks and critical infrastructure from the ever-growing threat of cyberattacks.

OMB Circular A-108, Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act (December 2016)

This circular describes agency responsibilities for implementing the review, reporting, and publication requirements of the Privacy Act of 1974 and related OMB policies.

Circular A-130: Managing Federal Information as a Strategic Resource (PDF, July 2016)

Information and IT resources are critical to the U.S. social, political, and economic well-being. They enable the federal government to provide quality services to citizens, generate and disseminate knowledge, and facilitate greater productivity and advancement as a nation. It is important for the federal government to maximize the quality and security of federal information systems and to develop and implement uniform and consistent information resources management policies in order to inform the public and improve the productivity, efficiency, and effectiveness of agency programs. Additionally, as technology evolves, it is important that agencies manage information systems in a way that addresses and mitigates security and privacy risks associated with new IT resources and new information processing capabilities.

M-16-17: OMB Circular A-123: Management's Responsibility for Enterprise Risk Management (ERM) and Internal Control (July 2016)

The policy changes in this circular modernize existing efforts by requiring agencies to implement an ERM capability coordinated with the strategic planning and strategic review process established by the Government Performance and Results Act Modernization Act (GPRAMA) and the internal control processes required by the Federal Managers' Financial Integrity Act (FMFIA) and the Government Accountability Office (GAO)'s Green Book. This integrated

governance structure will improve mission delivery, reduce costs, and focus corrective actions toward key risks.

Executive Order 13681: Improving the Security of Consumer Financial Transactions (PDF, October 2014)

This executive order requires agencies to strengthen the security of consumer data and encourage the adoption of enhanced safeguards nationwide in a manner that protects privacy and confidentiality while maintaining an efficient and innovative financial system.

Final Credentialing Standards for Issuing Personal Identity Verification (PIV) Cards under HSPD-12 (PDF, July 2008)

This memorandum provides final government-wide credentialing standards to be used by all federal departments and agencies in determining whether to issue or revoke PIV credentials to their employees and contractor personnel, including those who are non-United States citizens.

M-05-24: Implementation of HSPD-12 Policy for a Common Identification Standard for Federal Employees and Contractors (PDF, August 2005)

This memorandum provides implementation instructions for HSPD-12 and Federal Information Processing Standards (FIPS) 201.

HSPD-12: Policy for a Common Identification Standard for Federal Employees and Contractors (August 2004)

HSPD-12 calls for a mandatory, government-wide standard for secure and reliable forms of identification issued by the federal government to its employees and employees of federal contractors for access to federally controlled facilities and networks.

Standards

NIST SP 800-205: Attribute Considerations for Access Control Systems (PDF, June 2019)

This guideline provides federal agencies with information for implementing attributes in access control systems. Attributes enable a logical access control methodology where authorization to perform a set of operations is determined by evaluating attributes associated with the subject, object, requested operations, and, in some cases, environment conditions against policy, rules, or relationships that describe the allowable operations for a given set of attributes. This document outlines factors which influence attributes that an authoritative body must address when standardizing an attribute system and proposes some notional implementation suggestions for consideration.

NIST SP 800-116 Rev. 1: Guidelines for the Use of PIV Credentials in Facility Access (PDF, June 2018)

This guideline provides resources for using PIV credentials in facility access, enabling federal agencies to operate as government-wide interoperable enterprises. This guideline covers the risk-based strategy to select appropriate PIV authentication mechanisms as expressed within FIPS 201.

NIST SP 800-63-3: Digital Identity Guidelines (June 2017)

Agencies use these guidelines as part of the risk assessment and implementation of their digital service(s). These guidelines provide mitigations for an authentication error's negative impacts by separating the individual elements of identity assurance into its component parts.

NIST SP 800-63A: Digital Identity Guidelines - Enrollment and Identity Proofing (PDF, June 2017)

This guideline focuses on the enrollment and verification of an identity for use in digital services. Central to this is a process known as identity proofing in which an applicant provides evidence to a credential service provider (CSP) reliably identifying themselves, thereby allowing the CSP to assert that identification at an Identity Assurance Level (IAL). This document defines technical requirements for each of the three IALs.

NIST SP 800-63B: Digital Identity Guidelines - Authentication and Lifecycle Management (PDF, June 2017)

> These guidelines focus on the authentication of subjects interacting with government systems over open networks, establishing that a given claimant is a subscriber who has been previously authenticated. The result of the authentication process may be used locally by the system performing the authentication or may be asserted elsewhere in a federated identity system. This document defines technical requirements for each of the three Authentication Assurance Levels (AALs).

NIST SP 800-63C: Digital Identity Guidelines - Federation and Assertions (PDF, June 2017)

> These guidelines provide technical requirements for federal agencies implementing digital identity services and are not intended to constrain the development or use of standards outside of this purpose. This guideline focuses on the use of federated identity and the use of assertions to implement identity federations. Federation allows a given CSP to provide authentication and (optionally) subscriber attributes to a number of separately-administered relying parties. Similarly, relying parties may use more than one CSP.

NIST SP 800-73-4: Interfaces for PIV (PDF, February 2016)

> This guideline specifies the PIV data model, command interface, client application programming interface (API), and references to transitional interface specifications.

NIST SP 800-79-2: Guidelines for the Authorization of PIV Card Issuers (PCI) and Derived PIV Credential Issuers (DPCI) (PDF, July 2015)

> The guideline specifies the assessment for the reliability of issuers of PIV credentials and Derived PIV credentials. The reliability of an issuer is of utmost

importance when a federal agency is required to trust the identity credentials of individuals that were created and issued by another federal agency.

NIST SP 800-53 Rev. 5: Security and Privacy Controls for Federal Information Systems and Organizations (PDF, December 2020)

This guideline provides a catalog of security and privacy controls for federal information systems and organizations and a process for selecting controls to protect organizational operations, assets, individuals, other organizations, and the Nation from a diverse set of threats.

NIST SP 800-53A Rev. 4: Assessing Security and Privacy Controls in Federal Information Systems and Organizations - Building Effective Security Assessment Plans (PDF, December 2014)

This guideline provides a set of procedures for conducting assessments of security controls and privacy controls employed within federal information systems and organizations. The assessment procedures, executed at various phases of the system development lifecycle, are consistent with the security and privacy controls in NIST SP 800-53, Revision 4.

NIST SP 800-157: Guidelines for Derived PIV Credentials (PDF, December 2014)

This guideline provides technical instructions for the implementation of standards-based, secure, reliable, interoperable public key infrastructure (PKI) based identity credentials that are issued by federal departments and agencies to individuals who possess and prove control over a valid PIV credential.

NIST SP 800-162: Guide to Attribute Based Access Control (ABAC) Definition and Considerations (PDF, January 2014)

This guideline provides federal agencies with a definition of ABAC. ABAC is a logical access control methodology in which authorization to perform a set of operations is determined by evaluating attributes associated with the subject, object, requested operations, and, in some cases, environment conditions against

policy, rules, or relationships that describe the allowable operations for a given set of attributes.

FIPS 201-2: PIV of Federal Employees and Contractors (PDF, August 2013)

This standard specifies the architecture and technical requirements for a common identification standard for federal employees and contractors. The overall goal is to achieve appropriate security assurance for multiple applications by efficiently verifying the claimed identity of individuals seeking physical access to federally controlled government facilities and electronic access to government information systems.

NIST SP 800-76-2: Biometric Specifications for PIV (PDF, July 2013)

This guideline contains technical specifications for biometric data mandated in FIPS. These specifications reflect the design goals of interoperability and performance of the PIV credential. This specification addresses image acquisition to support the background check, fingerprint template creation, retention, and authentication. The biometric data specification in this document is the mandatory format for biometric data carried in the PIV Data Model (SP 800-73-1, Appendix A). Biometric data used only outside the PIV Data Model is not within the scope of this standard.

NIST SP 800-122: Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) (PDF. April 2010)

This guideline assists federal agencies in protecting the confidentiality of a specific category of data commonly known as PII. This document provides practical, context-based guidance for identifying PII and determining what level of protection is appropriate for each instance of PII. The document also suggests safeguards that may offer appropriate levels of protection for PII and provides recommendations for developing response plans for breaches involving PII.

Additional Resources

NIST FISMA Implementation Project: Risk Management Framework Overview (August 2020)

> The selection and specification of security controls for a system is accomplished as part of an organization-wide information security program that involves the management of organizational risk (that is, the risk to the organization or to individuals associated with the operation of a system). The management of organizational risk is a key element in the organization's information security program and provides an effective framework for selecting the appropriate security controls for a system (the security controls necessary to protect individuals and the operations and assets of the organization).

NIST SP 800-63 Frequently Asked Questions (FAQs) (July 2020)

> The Frequently Asked Questions for NIST SP 800-63-3: Digital Identity Guidelines answers recurring questions to provide additional clarification.

NIST SP 800-63-3 Implementation Resources (PDF, July 2020)

> These resources are intended as informative implementation guidance for NIST SP 800-63-3. These implementation resources provide guidance for SP 800-63-3 in three parts: Part A addresses SP 800-63A, Part B addresses SP 800-63B, and Part C addresses SP 800-63C.

NIST: Privacy Framework (PDF, January 2020)

> The Privacy Framework is a voluntary tool intended to help organizations identify and manage privacy risk to build innovative products and services while protecting individuals' privacy. The Privacy Framework approach to privacy risk is to consider privacy events as potential problems individuals could experience arising from system, product, or service operations with data, whether in digital or non-digital form, through a complete lifecycle from data collection through disposal.

NIST White Paper: Best Practices for Privileged User PIV Authentication (PDF, April 2016)

This white paper was developed in response to the Cybersecurity Strategy and Implementation Plan to explain the need for multifactor PIV-based user authentication for privileged users. It provides best practices for agencies implementing PIV authentication for privileged users.

Continuous Diagnostics and Mitigation

The Continuous Diagnostics and Mitigation (CDM) Program is an approach to fortifying the cybersecurity of government networks and systems. The CDM Program provides cybersecurity tools, integration services, and dashboards to participating agencies to support them in improving their respective security posture. The CDM approach focuses on five areas for the federal enterprise: Data Protection Management, Network Security Management, Identity and Access Management, Asset Management, and Monitoring and Dashboards.

Application Rationalization Playbook (PDF, June 2019)

This playbook is a practical guide for application rationalization and IT portfolio management under the federal government's Cloud Smart initiatives. Application rationalization will help federal agencies mature IT portfolio management capabilities, empower leaders to make informed decisions, and improve the delivery of key mission and business services. It requires buy-in from stakeholders across the enterprise, including senior leaders, technology staff members, cybersecurity experts, business leads, financial practitioners, acquisition and procurement experts, and end user communities. Rationalization efforts rely on leadership support and continual engagement with stakeholders to deliver sustainable change.