



National Security Agency/Central Support Service



# INFORMATION ASSURANCE DIRECTORATE

## CGS Identity Management Capability

Version 1.1.1

Identification is the means by which a user provides a claimed identity to the system. The most common form of identification is the user ID. A user ID is a unique identifier, such as a character string, used by an information system to identify a specific user. An identifier is a representation of a person (or non-person entities) on a network. A person or non-person entity can have more than one identifier.



# CGS Identity Management Capability



Version 1.1.1

## Table of Contents

1	Revisions.....	2
2	Capability Definition.....	3
3	Capability Gold Standard Guidance .....	3
4	Environment Pre-Conditions .....	5
5	Capability Post-Conditions .....	6
6	Organizational Implementation Considerations .....	6
7	Capability Interrelationships .....	8
7.1	Required Interrelationships .....	8
7.2	Core Interrelationships.....	8
7.3	Supporting Interrelationships.....	9
8	Security Controls.....	9
9	Directives, Policies, and Standards .....	12
10	Cost Considerations .....	17
11	Guidance Statements.....	18



# CGS Identity Management Capability



Version 1.1.1

## 1 Revisions

Name	Date	Reason	Version
CGS Team	30 June 2011	Initial release	1.1
CGS Team	30 July 2012	Inclusion of new IAD document template & Synopsis	1.1.1



# CGS Identity Management Capability



Version 1.1.1

## 2 Capability Definition

The Capability definition provides an understanding of the importance of the Capability to the Enterprise. It provides a high-level overview of the Capability based on definitions derived from Committee on National Security Systems (CNSS) Instruction No. 4009.

Identification is the means by which a user provides a claimed identity to the system. The most common form of identification is the user ID. A user ID is a unique identifier, such as a character string, used by an information system to identify a specific user. An identifier is a representation of a person (or non-person entities) on a network. A person or non-person entity can have more than one identifier.

Identity Management is the function that unambiguously associates identifiers with entities such as individuals, Organizations, Communities of Interest (COIs), automated processes, and devices—anyone or anything that can perform an action anywhere in the Enterprise system. Identity Management is the underpinning for building trust in a need-to-share Enterprise model, where entities in any environment (stable to austere), and from any location within an Enterprise system, will be able to access information, services, and communications resources based in large part on an authenticated identity. The Identity Management function provides the Enterprise with the ability to create, issue, distribute, maintain, archive, and manage the lifecycle of globally unique identifiers, as well as to serve as an authoritative source of identity information.

## 3 Capability Gold Standard Guidance

The Capability Gold Standard Guidance evaluates the Enterprise needs and overlays the expected Gold Standard behavior. The guidance goes beyond the concept of “good enough” when describing the Gold Standard recommendations, considers industry best practices, and describes a level of security that not only meets current standards but also exceeds them across the Enterprise.

The Identity Management Capability covers the full range of identity events, information, and documents, which includes verifying identity, issuing identity documents and credentials, and revoking identity. Identity Management is implemented through the process of identity creation, issue, distribution, maintenance, and archiving:

1. Creation—The Identity Management Capability within the Enterprise shall be able to validate and record identity evidence presented in support of an identity creation. Also, this Capability provides globally unique Identity References for each entity



# CGS Identity Management Capability



Version 1.1.1

(user and non-person entity such as device or service) in the Enterprise so that it is capable of functioning within a dynamic, federated, globally distributed Enterprise, including low bandwidth environments. Creation consists of three types of identifiers: unique identifiers, group identifiers, and aliases. Unique identifiers are created that conform to the Enterprise policy and are never reused. Group identifiers are handled as attributes or aliases (also known as identity designators). Aliases are openly acknowledged and identify what and who a person or non-person entity is. Identifying who the person or non-person entity is would be considered an Identity Reference (base identifier). The Capability shall be able to map which designators go with which references. In addition to openly acknowledged aliases, unacknowledged aliases shall be supported by creating two separate references. These references are mapped outside of the system.

2. Issue—The Identity Management Capability shall be able to issue and manage aliases, called identity designators, to users when required (e.g., a user known as “Mr. John Smith” may also require an identity designator of “Major John Smith, USMC”). Identity designators shall be mappable to an Identity Reference. There shall be a degree of confidence in the identity issuance process. For example, the lowest confidence level may begin with the user sending an email request to obtain certificates. A higher confidence model may require a more stringent process such as physical presence of the requester. This confidence level is supported by the identity proofing process in which credentials from other issuers are checked establish identity, enable interoperability, and record linkages to those other identities that the user has. The confidence levels, otherwise known as assurance levels, are defined by multiple policies according to agency. The Enterprise shall employ the highest assurance level in identity proofing as defined by the cognizant policy for that Enterprise. The confidence measure will include:
  - a. Considerations for the identity proofing processes used during the identity registration
  - b. The types of identity mechanisms
  - c. The strength of the identity mechanisms and the tokens that transfer them
  - d. The embodiment of the equipment used to access, transfer, and validate them
3. Distribution—Distribution includes the publishing of the identifier to the directory service, which shall be protected in accordance with System and Data Protection Capabilities. The directory service shall be centrally managed and serve as the authoritative source. The Enterprise shall have the ability to locate and use the authoritative source that will make identity values available to enable access decisions to be made. Logically, there is a single source of record that may be



# CGS Identity Management Capability



Version 1.1.1

distributed to other sources (source of reference). The only valid source is the individual or organization that provides the identifier (source of record, which is the authoritative source). Enterprises shall pull from the source of record, when validating an identifier.

4. Maintenance—Enterprises shall revalidate the status of the identifiers periodically (comparing human, non-human entities to see if the identifiers match the documented records and ensure the directory service is not out of date). In addition, Enterprises shall compare identifiers with other authoritative sources that are used to establish the identity, such as source databases or accreditation databases.
5. Archiving—An implementation of Identity Management shall include the ability to deactivate and remove an identifier from sources (directory services) it has been pushed to and create a deletion record with a time stamp. The Capability shall also be able to perform a universal update of the identifiers and will be based on credential and attribute updates (information is received from Credential or Attribute Management Capabilities). Universal updates shall be performed automatically, such that if an automated list is received from a system (e.g., personnel or member of a system), the Identity Management Capability shall be able to archive the groups of identifiers using batch processing methods.

Identities shall be managed throughout their lifecycle. Identities shall never be reused for different entities (e.g., if an Identity Reference is issued for “Captain Joe Smith,” that Identity Reference can never be assigned to a different user); therefore, all Identity References shall be unique. If the original “Captain Joe Smith” retires and years later a different “Captain Joe Smith” is assigned to the organization, this new person shall be assigned a unique Identity Reference. It is not acceptable to assign him the Identity Reference previously assigned to the different Captain.

## 4 Environment Pre-Conditions

The environment pre-conditions provide insight into environmental, user, and technological aspects needed for Capability implementation. These pre-conditions are services or other Capabilities that must be in place within the Enterprise for the Capability to function.

1. The Enterprise identifies the evidence required to enable the issuance of an Identity Reference for an individual and for a non-human entity, which will be based on the Organization’s associated policy.



# CGS Identity Management Capability



Version 1.1.1

2. Operating processes and governance ensures there is only one authoritative source per identifier.
3. Attribute management provides entity attributes.
4. Credential management provides Identity credentials.

## 5 Capability Post-Conditions

The Capability post-conditions define what the Capability will provide. They define functions that the Capability will perform or constraints that the Capability will operate under when performing its function.

1. The Capability will be able to register subject identities and issue, maintain, and archive globally unambiguous, assured identifiers.
2. All non-person entities within the Enterprise will have been assigned Identity References.
3. An Identity Reference will have provisions to specify the level of confidence of the identity proofing using metrics included in the associated policy.
4. The Capability uses standards-based Identity Management mechanisms to ensure interoperability across different platforms.
5. The Capability's Community-facing interfaces will be standard to ensure interoperability and promote information sharing. Elements have the option of choosing other interfaces for internal operations.
6. There will be only one globally unique Identity Reference for each authorized human and non-human entity that is part of, connects to, or operates over the Enterprise; non-human entities will not be issued ID designators.
7. Users or automated entities (non-person entities) will be registered within their elements using identity proofing that establishes a high degree of confidence in the subject's claimed identity.

## 6 Organizational Implementation Considerations

Organizational implementation considerations provide insight into what the Organization needs to establish, ensure, and have in place for the specified Capability to be effective. It provides guidance specific to the actions, people, processes, and departments that an Organization will need to execute or establish to implement the guidance described in Section 3 (Capability Gold Standard Guidance).

The Organization will ensure that all users and non-human identities are issued an identifier. The issuer of the identifier will provide the capability to generate and issue



# CGS Identity Management Capability



Version 1.1.1

identifiers, both human and non-person. Identifiers will be used to establish the users' identity within the Enterprise.

The Organization will ensure that authorized administrators provide a globally unique Identity Reference that serves as the foundation for distinguishing each principal (e.g., person, running application, hardware assets) from every other principal operating within the federated environment. The authorized administrator will validate the principal's credentials (e.g., driver's license, military ID, among others) provided from an authoritative source, such as a source of record, and associated identifiers.

The Organization will ensure that identity proofing of a user is performed prior to issuing an identifier and require the user to present evidence that is substantiated against information in the directory service. Sources of record will be authoritative or used for reference. In other words, the system may have to validate claimed identity by checking with an attribute authority elsewhere in Enterprise (e.g., Department of Motor Vehicles would be an authoritative source for driver's license credentials). Prior to being added to the system, all new users will have their identity verified to ensure the user is who he or she claims to be. Depending on the user's security level, this verification may require only original documentation (birth certificate, driver's license, social security card, etc.), or it may require a full background investigation.

Organizations will consider the following when using identifiers:

- Unique Identification—An Organization will require users to identify themselves uniquely before being allowed to perform any actions on the system unless user anonymity or other factors dictate otherwise.
- Maintenance of User IDs—An Organization will ensure that all user IDs belong to currently authorized users. Identification data will be kept current by adding new users.
- Inactive User IDs—User IDs that are inactive on the system for a specific period of time (e.g., 3 months) will be disabled.

When Identity Management is implemented correctly, the Organization will possess the capability to verify and track the unique identity of all entities (human and non-person entities) using each system. This unique identifier format will follow a convention that is based on the type of the entity (e.g., users are identified differently from hosts or services), which will be defined in such a way to allow for growth of the Organization and federation of identities.



# CGS Identity Management Capability



Version 1.1.1

## 7 Capability Interrelationships

Capability interrelationships identify other Capabilities within the Community Gold Standard framework that the Capability in this document relies on to operate. Although there are many relationships between the Capabilities, the focus is on the primary relationships in which the Capabilities directly communicate with or influence one another.

### 7.1 Required Interrelationships

The following Capability interrelationships include the other Capabilities within the Community Gold Standard framework that are necessary for the Capability in this document to operate.

- Personnel Security—The Identity Management Capability relies on the Personnel Security Capability to ensure that the identity of individuals has been verified prior to granting access to facilities, systems, and information.

### 7.2 Core Interrelationships

The following Capability interrelationships include the Capabilities within the Community Gold Standard framework that relate to every Capability.

- Portfolio Management—The Identity Management Capability relies on the Portfolio Management Capability to determine current and future investment needs and prioritize investments based on those needs.
- IA Policies, Procedures, and Standards—The Identity Management Capability relies on the IA Policies, Procedures, and Standards Capability to provide information about applicable federal laws, Executive Orders, regulations, directives, policies, procedures, and standards.
- IA Awareness—The Identity Management Capability relies on the IA Awareness Capability for an awareness program to inform personnel of their responsibilities related to IA.
- IA Training—The Identity Management Capability relies on the IA Training Capability to provide training programs related to IA activities in accordance with agency policies.
- Organizations and Authorities—The Identity Management Capability relies on the Organizations and Authorities Capability to establish the relevant roles and responsibilities.



# CGS Identity Management Capability



Version 1.1.1

## 7.3 Supporting Interrelationships

The following Capability interrelationships include the other Capabilities within the Community Gold Standard framework that are not necessary for the Capability to operate, although they support the operation of the Capability in this document.

- Data Protection–The Identity Management Capability relies on the Data Protection Capability to provide protection mechanisms for identifiers and identifying information.
- Risk Mitigation–The Identity Management Capability implements individual countermeasures that may be selected by the Risk Management Capability.

## 8 Security Controls

This section provides a mapping of the Capability to the appropriate controls. The controls and their enhancements are granularly mapped according to their applicability. In some instances, a control may map to multiple Capabilities.

Control Number/Title	Related Text
NIST SP 800-53 Revision 3, <i>Recommended Security Controls for Federal Information Systems and Organizations</i>	
AC-4 <i>INFORMATION FLOW ENFORCEMENT</i>	Control: The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy. Enhancement/s: (17) The information system: (a) Uniquely identifies and authenticates source and destination domains for information transfer; (b) Binds security attributes to information to facilitate information flow policy enforcement; and (c) Tracks problems associated with the security attribute binding and information transfer.
AU-10 <i>NON-REPUDIATION</i>	Control: The information system protects against an individual falsely denying having performed a particular action. Enhancement/s: (1) The information system associates the identity of the information producer with the information. (2) The information system validates the binding of the information producer's identity to the information.



# CGS Identity Management Capability



Version 1.1.1

	<p>(3) The information system maintains reviewer/releaser identity and credentials within the established chain of custody for all information reviewed or released.</p> <p>(4) The information system validates the binding of the reviewer's identity to the information at the transfer/release point prior to release/transfer from one security domain to another security domain.</p> <p>(5) The organization employs [Selection: FIPS-validated; NSA-approved] cryptography to implement digital signatures.</p>
<p>IA-2 IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)</p>	<p>Control: The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).</p> <p>Enhancement/s:</p> <p>(1) The information system uses multifactor authentication for network access to privileged accounts.</p> <p>(2) The information system uses multifactor authentication for network access to non-privileged accounts.</p> <p>(3) The information system uses multifactor authentication for local access to privileged accounts.</p> <p>(4) The information system uses multifactor authentication for local access to non-privileged accounts.</p> <p>(5) The organization:</p> <p>(a) Allows the use of group authenticators only when used in conjunction with an individual/unique authenticator; and</p> <p>(b) Requires individuals to be authenticated with an individual authenticator prior to using a group authenticator.</p> <p>(6) The information system uses multifactor authentication for network access to privileged accounts where one of the factors is provided by a device separate from the information system being accessed.</p> <p>(7) The information system uses multifactor authentication for network access to non-privileged accounts where one of the factors is provided by a device separate from the information system being accessed.</p> <p>(8) The information system uses [Assignment: organization-defined replay-resistant authentication mechanisms] for network access to privileged accounts.</p> <p>(9) The information system uses [Assignment: organization-</p>



# CGS Identity Management Capability



Version 1.1.1

	<p>defined replay-resistant authentication mechanisms] for network access to non-privileged accounts.</p>
<p><b>IA-3 DEVICE IDENTIFICATION AND AUTHENTICATION</b></p>	<p>Control: The information system uniquely identifies and authenticates [Assignment: organization-defined list of specific and/or types of devices] before establishing a connection.</p> <p>Enhancement/s:</p> <p>(1) The information system authenticates devices before establishing remote and wireless network connections using bidirectional authentication between devices that is cryptographically based.</p> <p>(2) The information system authenticates devices before establishing network connections using bidirectional authentication between devices that is cryptographically based.</p> <p>(3) The organization standardizes, with regard to dynamic address allocation, Dynamic Host Control Protocol (DHCP) lease information and the time assigned to devices, and audits lease information when assigned to a device.</p>
<p><b>IA-4 IDENTIFIER MANAGEMENT</b></p>	<p>Control: The organization manages information system identifiers for users and devices by:</p> <ol style="list-style-type: none"> <li>a. Receiving authorization from a designated organizational official to assign a user or device identifier;</li> <li>b. Selecting an identifier that uniquely identifies an individual or device;</li> <li>c. Assigning the user identifier to the intended party or the device identifier to the intended device;</li> <li>d. Preventing reuse of user or device identifiers for [Assignment: organization-defined time period]; and</li> <li>e. Disabling the user identifier after [Assignment: organization-defined time period of inactivity].</li> </ol> <p>Enhancement/s:</p> <p>(1) The organization prohibits the use of information system account identifiers as public identifiers for user electronic mail accounts (i.e., user identifier portion of the electronic mail address).</p> <p>4) The organization manages user identifiers by uniquely identifying the user as [Assignment: organization-defined characteristic identifying user status].</p> <p>(5) The information system dynamically manages identifiers,</p>



# CGS Identity Management Capability



Version 1.1.1

	attributes, and associated access authorizations.
IA-8 <i>IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)</i>	Control: The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users). Enhancement/s: None Specified
SC-20 <i>SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)</i>	Enhancement/s 1: (1) The information system, when operating as part of a distributed, hierarchical namespace, provides the means to indicate the security status of child subspaces and (if the child supports secure resolution services) enable verification of a chain of trust among parent and child domains.
SC-23 <i>SESSION AUTHENTICITY</i>	Control: The information system provides mechanisms to protect the authenticity of communications sessions. Enhancement/s: (1) The information system invalidates session identifiers upon user logout or other session termination. (2) The information system provides a readily observable logout capability whenever authentication is used to gain access to web pages. (3) The information system generates a unique session identifier for each session and recognizes only session identifiers that are system-generated. (4) The information system generates unique session identifiers with [Assignment: organization-defined randomness requirements].

## 9 Directives, Policies, and Standards

This section identifies existing federal laws, Executive Orders, regulations, directives, policies, and standards applicable to the Capability but does not include those that are agency specific.

Identity Management Directives and Policies

Title, Date, Status	Excerpt / Summary
Intelligence Community (IC)	



# CGS Identity Management Capability



Version 1.1.1

<p>Intelligence Community Public Key Infrastructure (PKI) Overarching Policy for the SCI Fabric, 25 October 1999, Classified</p>	<p>Summary: It is the policy of the Intelligence Community (IC) that a single-root, hierarchical Public Key Infrastructure (PKI) be established for use on Sensitive Compartmented Information (SCI) networks between members of the Community. The IC PKI will provide IC member Organizations, for those applications that require them, strong identification and authentication, data integrity, digital signature, non-repudiation, and encryption services for all information system-based communications and services traversing community SCI networks. These services shall be used for communications and services between IC member Organizations and those Organizations and their customers.</p>
<p>Intelligence Community Certificate Policy, Version 4.3.3, 25 September 2008, Classified</p>	<p>Summary: This policy provides uniform policy guidance and requirements for ensuring interoperability between Certification Authorities (CAs) within the IC PKI. It establishes standard operating policies and procedures to be used by IC agencies/components for services between members of the U.S. IC, IC customers, and others as approved by the Information and Technology Governance Board (ITGB) and the IC Chief Information Officer (CIO). IC PKI public certificates and associated private keys have applicability to areas such as, but not limited to, confidentiality of information, digital signatures, and identification and authentication of individuals, as well as information system infrastructure components.</p>
<p>ODNI/CIO-2009-310, Intelligence Community CIO Council Decisions Regarding IC Unique Identifiers for the Intelligence Community: Intelligence Community Digital Identifier (IC-ID) and Distinguished Name (DN), 26 August 2009, Classified</p>	<p>See CGS Classified Annex.</p>
<p>Intelligence Community Policy Guidance (ICPG)</p>	<p>See CGS Classified Annex.</p>



# CGS Identity Management Capability



Version 1.1.1

500.1, Digital Identity, 7 May 2010, Classified	
Comprehensive National Cybersecurity Initiative (CNCI)	
NSPD-54/HSPD-23 Cybersecurity Presidential Directive (Comprehensive National Cybersecurity Initiative [CNCI]), 8 January 2008, Classified	Summary: National Security Presidential Directive-54/Homeland Security Presidential Directive-23 (NSPD-54/HSPD-23), in which the Comprehensive National Cybersecurity Initiative (CNCI) is described, is classified. Initiative 7 deals with increasing the security of classified networks.
Department of Defense (DoD)	
DoD Directive 1000.25, DoD Personnel Identity Protection (PIP) Program, 23 April 2007, USD(P&R), Unclassified	Summary: The Personnel Identity Protection (PIP) shall be the Department of Defense's (DoD) program for ... establishing a secure and authoritative process for the issuance and use of identity credentials in the Department of Defense ... and ensuring that ... access to DoD physical and logical assets are granted based on authenticated and secure identity information. It establishes policy for the implementation and operation of the PIP program to include use of authoritative identity information, issuance and use of DoD identity credentials, ...
DODD 8320.03, Unique Identification (UID) Standards for a Net- Centric DoD, 23 March 2007, Unclassified	Summary: This standard requires the use of standardized Unique Identification (UID) for discrete entities throughout DoD and that UID standards will be based on the specific data, its associated attributes, the relationships of the data, and common Enterprise-wide capabilities.
DoD Instruction 8520.2, Public Key Infrastructure (PKI) and Public Key (PK) Enabling, 1 April 2004, Unclassified	Summary: This instruction implements policy, assigns responsibilities, and prescribes procedures for developing and implementing a department-wide PKI and enhancing the security of DoD information systems by enabling these systems to use PKI for authentication, digital signatures, and encryption. It aligns DoD PKI and PK-enabling activities with DoD Directive 8500.1, as implemented by DoD Instruction 8500.2, and the DoD Common Access Card (CAC) program, as specified by DoD Directive 8190.3.
Committee for National Security Systems (CNSS)	



# CGS Identity Management Capability



Version 1.1.1

Nothing found	
<b>Other Federal (OMB, NIST, ...)</b>	
Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, Version 1.0, 10 November 2009, Unclassified	Summary: This guidance outlines a common framework for identity, credential, and access management (ICAM) within the Federal Government and provides supporting implementation guidance for program managers, leadership, and stakeholders planning to execute a segment architecture for ICAM management programs. Includes courses of action, planning considerations, and technical solution information across multiple federal programs spanning the disciplines of ICAM. FICAM "offers an approach to identity management wherein creation and management of digital identity records are shifted from stove-piped applications to an authoritative Enterprise view of identity that enables application or mission-specific uses without creating redundant, distributed sources that are harder to protect and keep current."
<b>Executive Branch (EO, PD, NSD, HSPD, ...)</b>	
HSPD-12, Policy for a Common Identification Standard for Federal Employees and Contractors, 27 August 2004, Unclassified	Summary: U.S. policy is to enhance security, increase government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees). This directive mandates a federal standard for secure and reliable forms of identification.
EOP Memo M-05-24, Implementation of Homeland Security Presidential Directive (HSPD) 12, Policy for a Common Identification Standard for Federal Employees and Contractors, 5 August 2005, Unclassified	Summary: HSPD-12 requires the development and agency implementation of a mandatory, government-wide standard for secure and reliable forms of identification for federal employees and contractors. As required by the Directive, the Department of Commerce issued Federal Information Processing Standard (FIPS) 201 (the Standard). This memorandum provides implementing instructions for the Directive and the Standard.



# CGS Identity Management Capability



Version 1.1.1

Legislative	
Nothing found	

## Identity Management Standards

Title, Date, Status	Excerpt / Summary
Intelligence Community (IC)	
Intelligence Community Public Key Infrastructure (PKI) Interface Specification (Draft), Version 2.9.4, September 2009, Classified	Summary: This specification describes the interfaces to the IC PKI, defines the interface requirements for creating X.509 Version 3 (V3) certificates and X.509 Version 2 (V2) Certificate Revocation Lists (CRLs), provides a baseline for IC PKI certificate profiles (largely mirroring those of the DoD's PKI certificate profiles), and establishes the content for PKI certificates.
Comprehensive National Cybersecurity Initiative (CNCI)	
Nothing found	
Department of Defense (DoD)	
Nothing found	
Committee for National Security Systems (CNSS)	
Nothing found	
Other Federal (OMB, NIST, ...)	
FIPS 201-1 Personal Identity Verification (PIV) of Federal Employees and Contractors, March 2006, Unclassified	Summary: This standard specifies the architecture and technical requirements for a common identification standard for federal employees and contractors. Part one describes the minimum requirements for a federal personal identity verification (PIV) system that meets the control and security objectives of HSPD 12, including personal identity proofing, registration, and issuance. Part two provides detailed specifications that will support technical interoperability among PIV systems of federal departments and agencies.
NIST SP 800-76-1, Biometric Data Specification for Personal	Summary: This is a companion document to FIPS-201 that describes technical acquisition and formatting specifications for the biometric credentials of the PIV system, including the



# CGS Identity Management Capability



Version 1.1.1

Identity Verification (PIV), January 2007, Unclassified	PIV card itself. The primary design objective behind these particular specifications is high- performance universal interoperability.
Executive Branch (EO, PD, NSD, HSPD, ...)	
Nothing found	
Legislative	
Nothing found	
Other Standards Bodies (ISO, ANSI, IEEE, ...)	
Nothing found	

## 10 Cost Considerations

This section provides examples of some of the types of costs that the Organization will need to consider when implementing this Capability. The following examples are costs that are common across all of the Community Gold Standards Capabilities:

1. Solution used for implementation (hardware and/or software)
2. Necessary training
3. Licensing (if applicable)
4. Lifecycle maintenance
5. Impact/dependency on existing services
6. Manpower to implement, maintain, and execute
7. Time to implement, maintain, and execute
8. Network bandwidth availability and consumption
9. Scalability of the solution relative to the Enterprise
10. Storage and processing requirements

In addition to the common costs, the following are examples of cost considerations that are specific to this Capability:

1. The number of human and non-human entities—More entities to manage means more complex work and greater cost.
2. Licensing—There may be charges associated with connections to the authoritative source used for identity verification.



# CGS Identity Management Capability



Version 1.1.1

## 11 Guidance Statements

This section provides Guidance Statements, which have been extracted from Section 3 (Capability Gold Standard Guidance) of this Capability document. The Guidance Statements are intended to provide an Organization with a list of standalone statements that are representative of the narrative guidance provided in Section 3. Below are the Guidance Statements for the Identity Management Capability.

- The identity management system shall provide the Enterprise with the ability to create, issue, distribute, maintain, archive, and manage the lifecycle of globally unique identifiers, as well as to serve as an authoritative source of identity information.
- The identity management system shall be able to validate and record identity evidence presented in support of a creation.
- The identity management system shall provide a globally unique identity reference for each entity (user and non-person entity such as device or service).
- Identity creation shall consist of three types of identifiers: unique identifiers, group identifiers, and aliases.
- The identity management system shall issue and manage aliases (identity designators) to users, as necessary.
- The identity management system shall enforce confidence levels for issuing identities to users in accordance with Enterprise policy.
- The identity management system shall publish entity identifiers to the appropriate directory services.
- Directory services shall be centrally managed and serve as an authoritative source.
- The Enterprise shall have the ability to locate and use the authoritative source that will make identity values available to enable access decisions to be made.
- The Enterprise shall revalidate the status of the identifiers periodically to ensure the identifiers match the documented records and ensure the directory service is up to date.
- The Enterprise shall compare identifiers with other authoritative sources that are used to establish the identity, such as source databases or accreditation databases.
- The identity management system shall be able to deactivate or remove an identifier from sources (directory services) it has been pushed to and create a deletion record with a time stamp.
- The identity management system shall be able to perform a universal update to the identifiers based on credential and attribute updates.



# CGS Identity Management Capability



Version 1.1.1

- Universal updates of the identifiers, based on credential and attribute updates, shall be performed automatically.
- The identity management system shall be able to archive the groups of identifiers using batch processing methods.
- All identity references shall be unique and managed throughout their lifecycle and should never be reused for different entities.