



National Security Agency/Central Security Service



INFORMATION ASSURANCE DIRECTORATE

CGS Attribute Management Capability

Version 1.1.1

The Attribute Management Capability is responsible for managing the properties associated with entities in the Enterprise; these properties are referred to as attributes. An attribute represents the basic properties or characteristics of an entity that are used to enable the implementation of access control and configuration management policies.



CGS Attribute 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.....	5
6	Organizational Implementation Considerations	6
7	Capability Interrelationships.....	7
7.1	Required Interrelationships	8
7.2	Core Interrelationships	8
7.3	Supporting Interrelationships.....	8
8	Security Controls	9
9	Directives, Policies, and Standards	10
10	Cost Considerations	13
11	Guidance Statements.....	14



CGS Attribute 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 Attribute 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.

The Attribute Management Capability is responsible for managing the properties associated with entities in the Enterprise; these properties are referred to as attributes. An attribute represents the basic properties or characteristics of an entity that are used to enable the implementation of access control and configuration management policies. Examples of some possible attributes are contact attributes (email address, phone number), demographic attributes (organization, affiliation), and device attributes (physical location, logical addresses, installed software, and patch level).

Attribute Management encompasses the functions that manage the identification, maintenance, and publication of each attribute. In addition, Attribute Management identifies the attributes that are needed and an authoritative source from which to retrieve the attribute values.

A given attribute may be dynamic or static, which is determined by the authoritative source. Attribute Management provides for a capability in which all attributes stored by any system on a network are controlled by a set of policies to restrict or enable access based on functional need.

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.

Attribute Management provides for the publication of entity attributes to the Enterprise for use by people, devices, and services. The Capability exposes attributes maintained by authoritative sources that enable access decisions to be made. The Attribute Management function is responsible for identifying the location of the authoritative source. The Enterprise shall either be the authoritative source or it shall point to the authoritative source.



CGS Attribute Management Capability



Version 1.1.1

The Attribute Management Capability shall support the goal of a federated and interoperable attribute management system. The Capability shall support management of the attributes within the Enterprise, as well as management of the attributes for interoperability with other partners. In both instances, the attributes shall be centrally managed. Attribute Management is carried out by the identification, maintenance, and publishing of entity attributes.

Identification—Determines the attributes that are needed based on sensitivity levels, and identifies which authoritative sources provide the necessary attributes for entities. The Enterprise shall determine the appropriate authoritative source that will be used for access decisions. The Enterprise shall have the ability to locate and use the appropriate authoritative source that will make attribute values available to enable access decisions to be made.

Maintenance—Requires that the authoritative source be maintained and provide up-to-date attribute status information including attribute schemas for access management decisions. The Enterprise shall determine the refresh rate based on perishability of data, usually not to exceed 24 hours. If the authoritative source is not internal to the Enterprise, agreements shall be in place between the Enterprise and the authoritative source for refresh rates. The status of an attribute could change or the attribute could be a dynamic attribute; thus, every Enterprise shall perform attribute maintenance and ensure that an authorized source has an authorized person allowed to create, modify, and remove attributes that are no longer needed.

Publishing—Enables discovery and access of attributes for those users and systems that are authorized. The Enterprise shall ensure that an authorized source that is responsible for this function is accessible. Partner agreements shall be in place, and the Enterprise shall trust and share appropriate attributes with other enterprises as required for interoperability. Sensitivity shall dictate whether attributes are shown, allowed to be published, or the authoritative source is shown. The Organization shall make the attribute available based on the authority to see it. Every Enterprise shall either publish the authoritative source or show where to retrieve appropriate attribute information. The authoritative source shall enable access by maintaining a list of authorized users and systems. The source shall be updated as necessary and automated if possible.

The Attribute Management Capability exposes attributes to authorized users and non-person entities to enable searching. For devices, attributes such as physical location,



CGS Attribute Management Capability



Version 1.1.1

logical addresses, installed software, and patch level are created and maintained by multiple Community Gold Standard (CGS) Capabilities but exposed to the Enterprise through Attribute Management. The Gold Standard for Attribute Management allows attributes to be created and maintained for use in configuration management decisions.

Mission stakeholders and data owners within the Enterprise shall identify the appropriate attributes used to determine an entity's authorization based on role, function, mission supported, and policy. To achieve the functions required by Attribute Management, the Capability shall be fully implemented with Identity Management, Credential Management, Access Management, and other system entities so that it can efficiently obtain and distribute the information required.

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. Identity management has established a source of identities.
2. Secured infrastructure exists for Attribute Management systems.
3. Established source(s) of record exists.
4. Established trust and processes for interoperability sharing exists.
5. Access management has established rules for use of attributes.
6. Digital policy has been established to manage the definition and collection of attributes.

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 allows for all attributes to have an authoritative source to enable the Access Management Capability to locate attributes and make decisions.
2. The Capability allows for all users and entities to have attributes for use in access control decisions.
3. The Capability allows for attributes to be identified, maintained, and published.
4. The Capability enables sharing based on policy. This Capability is not responsible for establishing this policy.



CGS Attribute Management Capability



Version 1.1.1

5. The Capability allows Configuration Management to use attributes to configure devices. Configurations themselves may also be attributes.
6. The Capability allows for the management of non-access-based attributes.

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).

When the Attribute Management Capability is implemented correctly, the Organization will possess a capability to verify the attributes to support identity decisions of each of its entities (user and non-person) and work with Access Management to ensure the attributes are used to make access control decisions.

Each Organization will determine what attributes are required and identify the authoritative source for those attributes. The authoritative source will store the attributes and provide up-to-date and reliable attribute values. The Organization will support management of the attributes within the Enterprise, as well as management of the attributes for interoperability with other partners. The Organization will provide central management in both instances. If an Organization has to identify attributes and there is no authoritative source, the Organization will need to decide whether to remove the attributes.

Attribute Management provides attributes that are leveraged by Access Management to determine whether an entity is permitted to perform an action. The Organization will ensure entity attributes are published to an authoritative source for use by people, devices, and services. The authoritative source will assist the Access Management Capability in determining whether the requesting entity possesses the attributes (e.g., roles, clearance, organizational affiliation, cryptographic mechanisms) to satisfy the conditions imposed by the digital policy. If so, the entity will be permitted to perform a specified action.

Each Organization will ensure that attributes are under configuration control and develop a policy for retiring attributes that are no longer needed. Policy will be created and enforced by the Organization that defines who will retire attributes.



CGS Attribute Management Capability



Version 1.1.1

The Organization will designate an authoritative source that is responsible for removing attributes from user and non-person entities. When an attribute is retired, the Organization will ensure that expected values are not missing. The authoritative source will leverage Digital Policy and work with Access Management to communicate when an access is no longer needed. If the authoritative source is not internal, but Digital Policy is within the Organization, the Organization will communicate with the external organization that maintains the authoritative source to ensure the updates occur. The authoritative source will be updated as necessary and automatically if possible.

Many different types of attributes may be created, modified, and removed frequently. Keeping track of all these attributes in any manner is challenging. To assist in this effort, when each system creates a new attribute, each Organization will ensure that the authoritative source logs the change and performs updates accordingly for all new, modified, and removed attributes. The Community Gold Standard does not dictate how often the data will be refreshed; however, typical refresh rates do not exceed 24 hours. Caching of attributes will not be allowed unless mission needs dictate so (e.g., disconnected operations).

Organizations will ensure that an authoritative source shares attributes with only authorized entities through the definition of policies that will be used to define access control. Only necessary services or users are permitted access to attributes. Those who are permitted will have access to only those attributes required to fulfill their functional task. Each Organization will enforce access control policies to prevent unauthorized access. In addition, all systems that store attributes have system availability requirements. Organizations will ensure redundant systems are in place for systems providing attribute information.

The Organization will use attributes for device configuration management. Asset attributes such as physical location, logical addresses, installed software, and patch level will be created and maintained by other Capabilities and exposed to the Enterprise through Attribute Management for use in configuration management decisions.

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



CGS Attribute Management Capability



Version 1.1.1

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.

- Digital Policy Management—The Digital Policy Management Capability relies on the Attribute Management Capability to provide attributes associated with entities and resources that are used to determine applicability of digital policies.
- Metadata Management—The Attribute Management Capability relies on the Metadata Management Capability to tag assets with attributes that take the form of IA metadata.

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 Attribute 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 Attribute 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 Attribute Management Capability relies on the IA Awareness Capability for an awareness program to inform personnel of their responsibilities related to IA.
- IA Training—The Attribute 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 Attribute Management Capability relies on the Organizations and Authorities Capability to establish the relevant roles and responsibilities

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.



CGS Attribute Management Capability



Version 1.1.1

- System Protection–The Attribute Management Capability relies on the System Protection Capability to protect the systems that store attribute data.
- Communication Protection–The Attribute Management Capability relies on the Communication Protection Capability to protect attribute data when in transit.
- Personnel Security–The Attribute Management Capability relies on Personnel Security to provide clearance information, which may be used as attributes for access decisions.
- Data Protection–The Attribute Management Capability relies on the Data Protection Capability to provide protection mechanisms for attributes.
- Risk Mitigation–The Attribute Management Capability implements individual countermeasures that may be selected by the Risk Mitigation 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.
AC-16 <i>SECURITY ATTRIBUTES</i>	Control: The information system supports and maintains the binding of [Assignment: organization-defined security attributes] to information in storage, in process, and in transmission. Enhancement/s:



CGS Attribute Management Capability



Version 1.1.1

	<p>(1) The information system dynamically reconfigures security attributes in accordance with an identified security policy as information is created and combined.</p> <p>(2) The information system allows authorized entities to change security attributes.</p> <p>(3) The information system maintains the binding of security attributes to information with sufficient assurance that the information--attribute association can be used as the basis for automated policy actions.</p> <p>(4) The information system allows authorized users to associate security attributes with information.</p> <p>(5) The information system displays security attributes in human-readable form on each object output from the system to system output devices to identify [Assignment: organization-identified set of special dissemination, handling, or distribution instructions] using [Assignment: organization-identified human readable, standard naming conventions].</p>
<p>IA-4 IDENTIFIER MANAGEMENT</p>	<p>Enhancement/s:</p> <p>(5) The information system dynamically manages identifiers, attributes, and associated access authorizations.</p>

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.

Attribute Management Directives and Policies

Title, Date, Status	Excerpt / Summary
Intelligence Community (IC)	
ICPM 2007-500-3, Intelligence Information Sharing, 22 December 2007, Unclassified	<p>Excerpt: D.5. To maximize the dissemination of intelligence information to Intelligence Community (IC) customers relevant to their missions, while balancing the obligation to protect intelligence sources and methods, the IC elements shall:</p> <p>c. Implement a Director of National Intelligence (DNI) approved attribute-based Identity Management Capability to enable attribute-based access, user authorization, and</p>



CGS Attribute Management Capability



Version 1.1.1

	user auditing services.
Intelligence Community (IC) Design Patterns, Identity and Access Management (IdAM) Design Patterns, Version 0.9, 15 January 2010, Unclassified	Summary: This document provides solution options for attribute sharing as a community resource, a shared resource, and a local resource. These options will be supported at network boundaries where element networks will connect to the federated IC Enterprise.
ICD 501, Discovery and Dissemination or Retrieval of Information within the Intelligence Community, 21 January 2009, Unclassified	Excerpt: F.2. When seeking to obtain discovered information that the steward has not preapproved for retrieval, authorized IC personnel shall provide the steward with information regarding their role, assigned mission need, and when established, DNI-approved identity attributes.
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)	
DODD 8320.03, Unique Identification (UID) Standards for a Net-Centric DoD, 23 March 2007, Unclassified	Summary: This directive requires the use of standardized Unique Identification (UID) for discrete entities throughout the Department of Defense (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.
Committee for National Security Systems (CNSS)	
Nothing found	
Other Federal (OMB, NIST, ...)	
Federal Identity, Credential, and Access Management (FICAM)	Summary: This guidance outlines a common framework for Identity, Credential, and Access Management (ICAM) within the Federal Government and provides supporting



CGS Attribute Management Capability



Version 1.1.1

Roadmap and Implementation Guidance, Version 1.0, 10 November 2009, Unclassified	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 establishes a strong relationship between attributes and identity and identity management.
Executive Branch (EO, PD, NSD, HSPD, ...)	
Nothing found	
Legislative	
Nothing found	

Attribute Management Standards

Title, Date, Status	Excerpt / Summary
Intelligence Community (IC)	
Nothing found	
Comprehensive National Cybersecurity Initiative (CNCI)	
Nothing found	
Department of Defense (DoD)	
IC/DoD Unified Authorization and Attribute Service (UAAS) Authorization Attribute Set, v0.4, 14 April 2008, Classified	Summary: This document defines a set of subject attributes used to support Attribute-Based Access Control (ABAC) decisions across the DoD and IC. It provides a catalog of attribute names and values harmonized across the primary networks: Unclassified but Sensitive Internet Protocol Router Network (NIPRNet), Secret Internet Protocol Router Network (SIPRNet), and the Joint Worldwide Intelligence Communications System (JWICS); and it specifies the subset of attributes required to be available to mission systems on each of those networks.
Committee for National Security Systems (CNSS)	



CGS Attribute Management Capability



Version 1.1.1

Nothing found	
Other Federal (OMB, NIST, ...)	
Nothing found	
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. Number of entities (users, devices, etc.)—The number of attributes and the number of entities these attributes need to be associated with will affect the cost of operating this Capability.
2. Solution used for implementation—The solution used for managing attributes will need to be able to scale as the Enterprise grows.



CGS Attribute 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 Attribute Management Capability.

- The Enterprise shall manage the properties associated with entities in the Enterprise; these properties are referred to as attributes. An attribute represents the basic properties or characteristics of an entity that are used to enable the implementation of access control and configuration management policies.
- The Enterprise shall establish an attribute management system to provide for the publication of entity attributes for use by people, devices, and services.
- The attribute management system shall be responsible for identifying the location of the authoritative source. The Enterprise shall be the authoritative source or it shall point to the authoritative source.
- The attribute management system shall support management of attributes within the Enterprise and across Enterprise boundaries.
- The attribute management system shall be centrally managed.
- The attribute management system shall determine the attributes that are needed based on sensitivity levels.
- The attribute management system shall identify which authoritative sources provide the necessary attributes for entities.
- The Enterprise shall determine the appropriate authoritative sources that will be used for access decisions.
- The Enterprise shall have the ability to locate and use the appropriate authoritative source that will make attribute values available to enable access decisions to be made.
- The attribute management system shall maintain requisite access to authoritative sources for up-to-date attribute status information.
- The Enterprise shall determine the refresh rate based on perishability of data.
- The Enterprise shall establish agreements with authoritative sources for refresh rates when the authoritative source is external to the Enterprise.
- The Enterprise shall perform attribute maintenance and ensure that an authorized source has an authorized person allowed to create, modify, and remove attributes that are no longer needed.
- The attribute management publishing service shall enable discovery and access to attributes by authorized users and systems.



CGS Attribute Management Capability



Version 1.1.1

- The Enterprise shall ensure that an authorized source that is responsible for publishing is accessible.
- The Enterprise shall establish partner agreements with other Enterprises as required for interoperability.
- The Enterprise shall manage the properties associated with entities in the Enterprise; these properties are referred to as attributes. An attribute represents the basic properties or characteristics of an entity that are used to enable the implementation of access control and configuration management policies.
- Sensitivity shall dictate whether attributes are shown or allowed to be published, or the authoritative source is shown. The Enterprise shall make the attribute available based on the authority to see it.
- The Enterprise shall either publish the authoritative source or show where to retrieve the appropriate attribute information.
- The attribute management system shall enable access by maintaining a list of authorized users and systems.
- Publishing of attributes shall be updated as necessary and shall be automated, where possible.
- The attribute management system shall expose attributes to authorized users and non-person entities to enable searching.
- Mission stakeholders and data owners within the Enterprise shall identify the appropriate attributes used to determine an entity's authorization based on role, function, mission supported, and policy.
- The Enterprise shall have an identity management, credential management, and access management system that it can use to execute necessary attribute management-related actions.