TLP:CLEAR

CONTINUOUS DIAGNOSTICS AND MITIGATION PROGRAM

Identity, Credential, and Access Management (ICAM) Reference Architecture

Version: 1.3

Publication: September 2023

Cybersecurity and Infrastructure Security Agency

TLP:CLEAR

REVISION HISTORY

Version	Summary of revisions	Date
1.0	Initial release	09/08/2021
1.1	Added Non-Person Entity (NPE) information	01/27/2022
1.2	Added cloud information	07/18/2022
1.3	Added Zero Trust information	09/12/2023

CONTENTS

1. EXECUTIVE SUMMARY

There is no singular, authoritative, recognized way to architect an Identity, Credential, and Access Management (ICAM) capability across an enterprise, which results in many U.S. government agencies addressing this critical capability from different directions with different priorities. Compounding this issue, the maturity level of Identity Management varies across agencies , especially as related to tool expertise and ICAM-related policies, which may complicate ongoing CDM integration efforts and lead to incomplete or ineffective ICAM deployments.

This document refines and clarifies the CDM Program's Identity and Access Management (IDAM) scope by providing a reference for how CDM IDAM capabilities may integrate into an agency's ICAM architecture. A description of the federal ICAM practice area, including how ICAM services and components implement ICAM use cases, is provided, along with a description of related CDM capabilities. For each CDM ICAM capability, assumptions and constraints are made in reference to agency capabilities.

Figure ES-1 summarizes the CDM IDAM capabilities (left) and the related federal ICAM (FICAM) practice areas and services (right) diagram and highlights that both users and devices need to be considered in Access Management. CDM CRED (Manage Credentials and Authentication), BEHAVE (Manage Security-Related Behavior), TRUST (Manage Trust in People Granted Access), and PRIV (Privilege Management) all collect desired and actual states. The actual state shows the respective capabilities and comparing the desired state and actual state allows reporting of defects.

CDM IDAM capabilities have evolved since initial implementations to include sub-capabilities for Privileged Access Management (PAM) and Identity Lifecycle Management (ILM) under the PRIV capability area and Mobile Identity Management (MIM) under the CRED capability area. CRED has evolved to include non-person entities (NPE) and other non-PKI authenticators beyond the original, which was focused on Personal Identity Verification (PIV) credentials.

Functionality in the PAM sub-capability is focused on ensuring that privileged human and non-person entities are managed separately from unprivileged users and provides tools to assist with ensuring strong authentication where modern methods are not natively available. PAM sub-capability provides a Policy Decision Point (PDP) and a Policy Enforcement Point (PEP) for privileged user Access Management. PDPs and PEPs play an essential role in ensuring policies are enforced in both legacy and cloud environments. PDPs and PEPs are central within ICAM's "Access Management" service area, which we will expand upon herein.

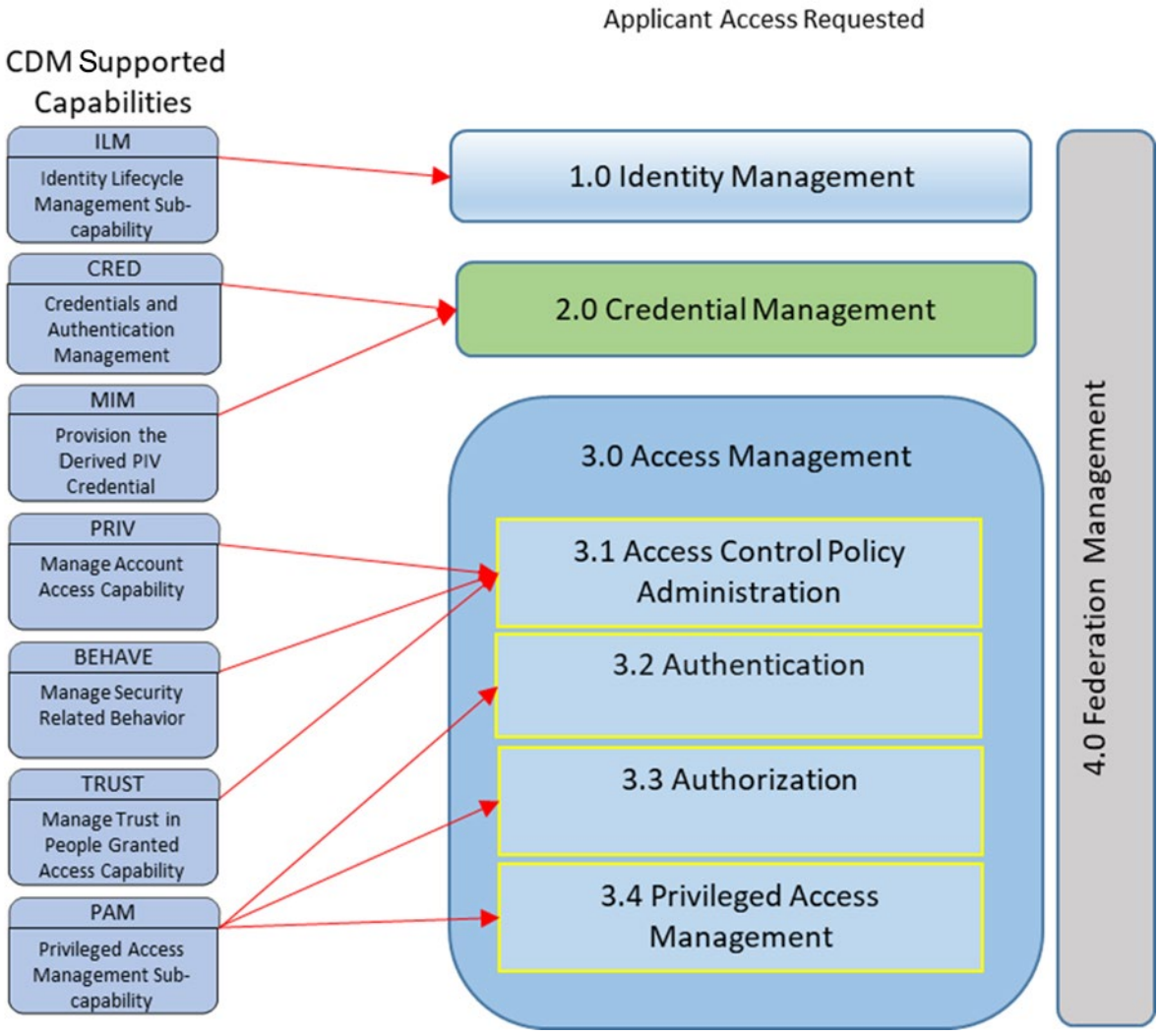
Functionality in the ILM sub-capability is focused on the lifecycle management of a user's identity and their associated privileges throughout the user's association with the agency. Although ILM applies to all users, human and non-person, in an enterprise, CDM takes a particularly focused view on ILM in relation to privileged users because these are the most powerful and abused and therefore require closer evaluation throughout the identity lifecycle.

MIM is a sub-capability under CRED that enables an agency to secure users the use of mobile devices. The MIM capability participates in the Derived Personal Identity Verification (PIV) Credentials (DPC) lifecycle through the Enterprise Mobility Manager. DPC lifecycle includes issuance, renewal, reissuance, activation and deactivation, and revocation and deletion events. It also supports the provisioning of derived PIV credentials for mobile devices.

In this architecture, we introduce federation services. In a manner similar to PDPs and PEPs used in the PAM sub-capability, Federation services are an extension of Access Management and rely on PDPs and PEPs to operate. Federation services include additional service endpoints, the Identity Provider (IDP), which is responsible for the authentication event, and the relying party (RP) (aka Service Provider), which provides

access to the service itself. The service expectations are defined in federation agreements between the parties.

Zero Trust is a cybersecurity model for a network architecture that implicitly trusts no device or user by default, authenticating every transaction. The federal government has released much guidance on Zero Trust Architecture (ZTA) and has called for its implementation on federal networks. This CDM ICAM Reference Architecture addresses ZTA and illustrates how ICAM and CDM help enable it.



HWAM: Hardware Asset Management; SWAM: Software Asset Management; VUL: Vulnerability Management

Figure ES-1: Top-Level CDM ICAM Functional Block Diagram

2. INTRODUCTION

The CDM Program deploys Information Security Continuous Monitoring (ISCM)[1] capabilities, including monitoring, diagnostics, and mitigation capabilities designed to strengthen the security posture of federal .gov networks. CDM supports ICAM with its Identity and Access Management (IDAM) capability area. This CDM ICAM reference architecture can be used as an authoritative source for architecting a robust and effective ICAM capability that includes CDM functionality.

There is no singular, authoritative, recognized way to architect an ICAM capability across an enterprise, which results in many U.S. government agencies approaching this from different directions with different priorities. Compounding this issue, agency Identity Management maturities vary, especially those related to tool expertise and ICAM-related policies, which may complicate the ongoing CDM integration efforts and lead to incomplete or ineffective ICAM deployments.

2.1 PURPOSE

This document refines and clarifies the CDM Program's Identity and Access Management (IDAM) scope by providing a reference for how CDM IDAM capabilities may integrate into an agency's ICAM architecture. CDM stakeholders interested in CDM ICAM capabilities and how they integrate with agency Federal Identity, Credential, and Access Management (FICAM) components are the intended readership for this document.

The CDM ICAM reference architecture described herein consists of CDM IDAM capability area functions and references FICAM architecture functions external to CDM.[2] The interfaces and data flows between CDM and external FICAM functions are described.

This document does not cover the details of a physical interface between CDM and other FICAM components because the interface can differ across agencies. The document does, however, provide a high-level notional physical implementation.

2.2 DOCUMENT OVERVIEW

This remainder of this document is organized as follows:

- Section 3 provides a list of assumptions.
- Section 4 provides an overview of the CDM architecture, with a focus on the IDAM capability area.
- Section 5 contains an overview of a reference FICAM architecture into which CDM expects to incorporate processes and data when integrating at an agency. It also describes concepts such as cloud, Zero Trust, governance, and federation as applied to the ICAM community.
- Section 6 describes the integration of CDM into the reference FICAM architecture or into the ICAM reference architecture.
- Section7 provides a notional physical architecture for integration of CDM into the FICAM architecture at the agency.
- Section 8 considers some challenges associated with the integration of CDM and agency FICAM functions.
- Appendix A is a bibliography of relevant publications used in this document.
- Appendix B provides a glossary of terms as applied to FICAM.

[1] National Institute of Standards and Technology (NIST) Special Publication (SP) 800-137 [Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organization] guidance defines ISCM as "maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions."
[2] General Services Administration, "The Federal Identity, Credential, and Access Management Architecture," Version 3.1, FINAL, January 6, 2021, accessed May 20, 2022, https://playbooks.idmanagement.gov/docs/ficam-arch.pdf.

- Appendix C defines the acronyms used in this document.

3. ASSUMPTIONS

The following list of assumptions applies in this document.

- CDM functionality described herein is based on the 2023 CDM Technical Volume 2 requirements as currently accepted into the CDM Requirements Management System.
- Updates to the IDAM capability area in CDM Technical Volume 2 may impact the CDM ICAM Reference Architecture.
- CDM IDAM capabilities are applicable to authorized employees and contractors. Other human users such as mission partners and constituents are not part of the targeted capabilities of CDM at this time.
- For the purpose of the CDM ICAM reference architecture, the focus is on human users [person entities (Pes)] in all cases and non-person entities (NPEs) that are considered privileged.
- The CDM ICAM reference architecture addresses Zero Trust Architecture (ZTA), including what impacts, if any, it has on CDM capabilities and functions.

In-scope NPEs can include devices, software applications, and processes that have accounts used to access agency systems. An NPE would be under the control of an authorized PE who has the ability to create, modify, or destroy the NPE account. Assumptions directly related to the CDM ICAM reference architecture are provided in Section 6.

4. CDM OVERVIEW

4.1 CDM ARCHITECTURE

The CDM system architecture employs a layered approach, as shown in Figure 4-1. CDM is composed of a tools and sensor level (A), an integration level (B), an Agency Dashboard level (C), and a Federal Dashboard level (D). CDM provides asset management, IDAM, network security management, and data protection management capabilities.

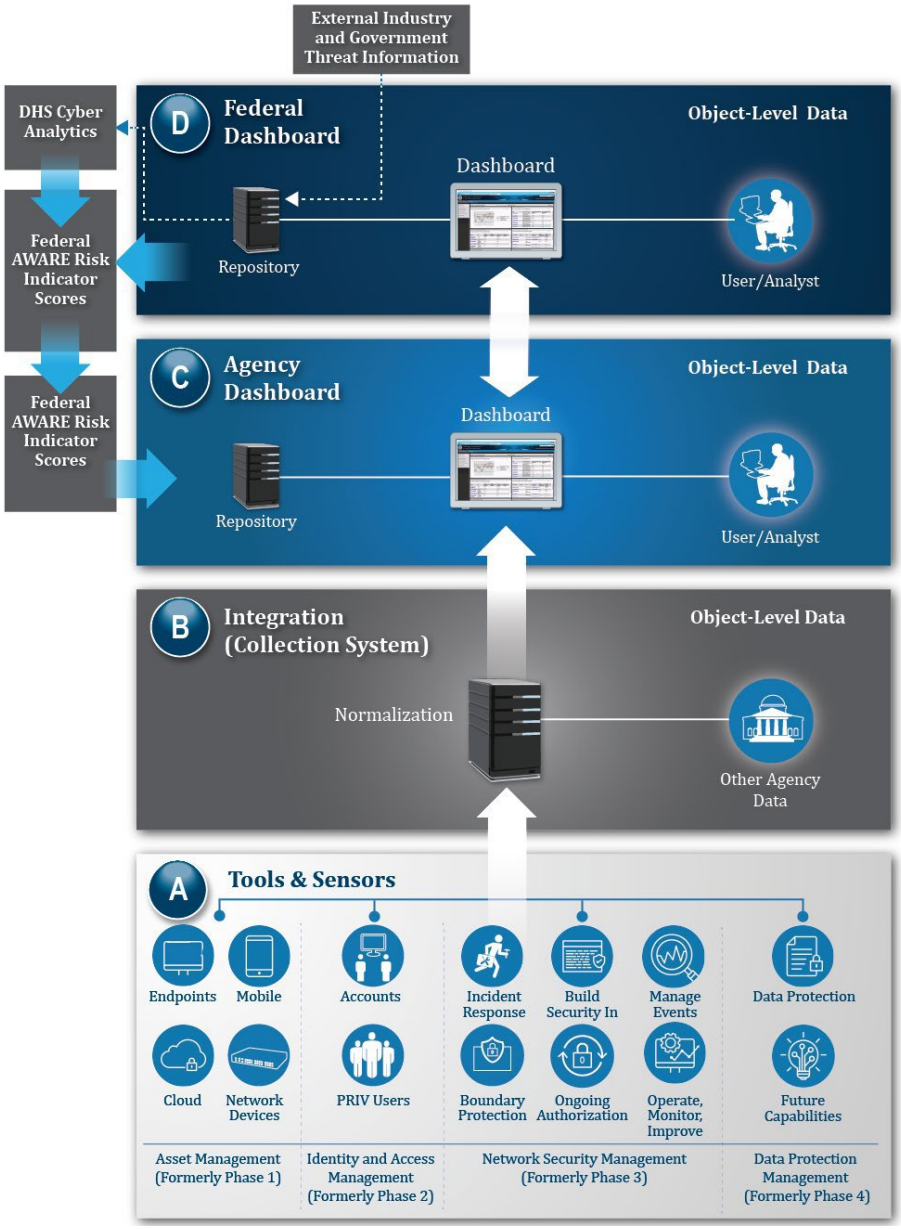


Figure 4-1: CDM Systems Architecture

Information from CDM sensors deployed in the agency network is normalized and aggregated, then sent to the Agency Dashboard, where it is stored and made available to agency analysts. In the event that agencies are leveraging existing sensors, those sensors also feed data into the Agency Dashboard. Agencies have the option to deploy a more complex structure of dashboards.

Agency dashboards include information on specific CDM objects and defect checks, as well as risk-scoring information for the agency. The Agency Dashboard stores, processes, and displays the lowest level of information about the cybersecurity posture gaps detected in each agency's Information Technology (IT) assets. The Agency Dashboards prioritize the most serious problems and allow analysts to investigate the specifics for each reported risk. The dashboard gives technical managers insight into risks present in the systems and networks under their responsibility. Additionally, it provides executive managers an aggregated view of risks. Its functionality allows each level of manager to investigate risks under their purview and examine the details to identify who has responsibility for each risk.

All agencies that participate in the CDM Program are required to provide automatic federal and summarized data feeds from their dashboards to the Federal Dashboard. The data flow between the CDM Agency and Federal dashboards is bi-directional, indicating that both dashboards share information with each other. The CDM Agency Dashboard receives, aggregates, and displays information from CDM tools on agency networks. It provides operational visibility of object-level CDM data for the CISA analysts using the CDM Federal Dashboard in support of Executive Order 14028.

4.2 CDM CAPABILITIES

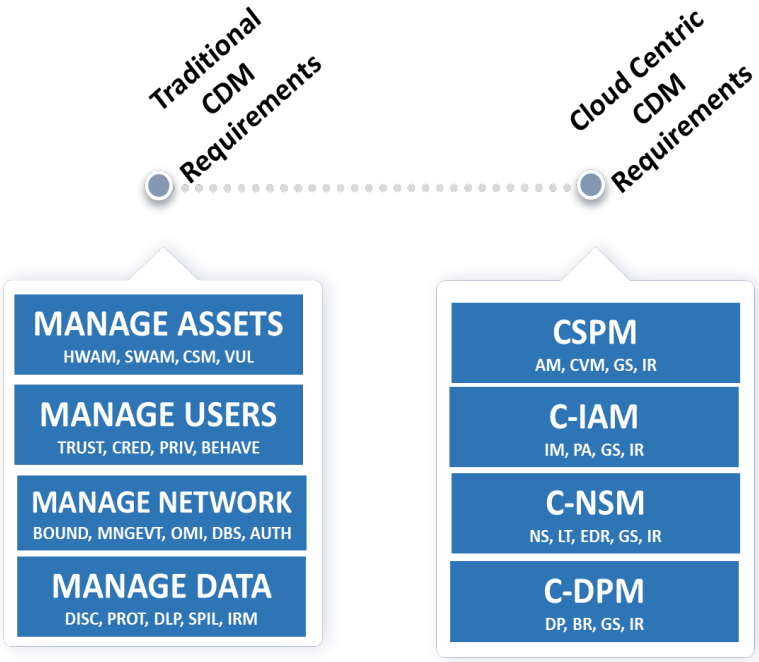
To fulfill its mission, the CDM Program provides the capabilities identified in Table 4-1. The focus of the FICAM reference architecture is on the IDAM capability area (shaded rows in the table).

Table 4-1: CDM Capabilities by Capability Area

CDM Capabilities	Description
Asset Management	
Manage Hardware Inventory (HWAM)	HWAM discovers and manages Internet Protocol (IP)-addressable devices on the network.
Manage Software Inventory (SWAM)	SWAM discovers software installed on managed network hardware devices.
Manage Configuration Settings (CSM)	CSM automatically and continuously verifies that the *authorized security configuration benchmarks* (and *relevant configurable settings)* are applied to agency assets.
Manage Vulnerabilities (VUL)	VUL discovers and identifies *known software mistakes and deficiencies* that a hacker can use to gain access to a system or network.
Identity and Access Management	
Enterprise Mobility Management (EMM)	EMM is a suite of services and technologies that enables an agency to secure the use of mobile devices (such as tablets, smartphones, and e-readers) per the agency's policies and identifies *instances of non-compliance with agency policy for mobile devices.*
Manage Trust in People Granted Access (TRUST)	TRUST monitors vetted trust level and identifies *instances in which an authorized user does not comply with agency policy on TRUST.*
Manage Security-Related Behavior (BEHAVE)	BEHAVE ensures authorized users exhibits the appropriate behavior for their role and identifies *instances in which an authorized user does not comply with agency policy on training, user agreements, or other agency-defined requirements*.
Manage Credentials and Authentication (CRED)	CRED ensures account credentials are assigned to, and only used by, authorized users or services and identifies *instances in which an authorized user's credentials do not comply with agency policy*.
Mobile Identity Management (MIM)	A sub-capability under CRED, MIM enables an agency to secure the use of mobile devices by provisioning a derived personal identity verification (PIV) credential.
Privilege Management (PRIV)	PRIV provides the agency with insight into risks associated with *authorized users not complying with related agency policy or being granted excessive privileges* to systems and information at any level of sensitivity.
Privileged Access Management (PAM)	A sub-capability under PRIV, PAM provides a Policy Enforcement Point (PEP) for privileged user Access Management, primarily for administrators.
Identity Lifecycle Management (ILM)	A sub-capability under PRIV, ILM adjusts information in connected repositories to address changing privileged user positions and responsibilities.
Network Security Management	
Boundary Protection (BOUND)	This capability provides network boundary protections that support the network security management key program area.
Manage Events (MNGEVT)	This capability gathers threat data from appropriate sources, *identifies security incidents* through analysis of data, and performs initial vulnerability assessment impact analyses.
Operate, Monitor, and Improve (OMI)	This capability is responsible for performing detailed investigation of security incidents.

CDM Capabilities	Description
Design and Build in Security (DBS)	This capability supports cybersecurity practices for developing and deploying software and systems throughout the engineering lifecycle.
Data Protection Management	
Data Discovery / Classification (DATA_DISCOV)	This capability supports consistent identification of "data assets" across the organization for processing, storing, and transmitting information at all sensitivity levels.
Data Protection (DATA_PROT)	This capability provides data protection functions to ensure the confidentiality and integrity of data.
Data Loss Prevention (DATA_DLP)	This capability provides data protection and integrity functions through automated data loss prevention capabilities.
Information Rights Management (DATA_IRM)	This capability provides data protection through information rights management capabilities.

CDM cloud capabilities will be added as they are developed. The CDM Cloud Guidance Document Volumes 1 and 2 provide CDM-relevant architectures, data flows, and data sources in cloud environments. Based on the guidance documents, the draft CDM Cloud Requirements Catalog with requirements for Cloud Security Posture Management (CSPM) was developed, and Figure 4-2 was used to show the traditional CDM capabilities and how they are to be represented in CDM cloud concepts. On the right side of the diagram, C-IAM is the Cloud Identity and Asset Management, C-NSM is the Cloud Network Security Management, and C-DPM is the Cloud Data Protection Management.



Acronyms not previously defined or defined within the figure can be found in Appendix C.

Figure 4-2: CDM Capability Areas Related to Cloud Security Function Groups[3]

The CDM cloud guidance documents relating to C-IAM highlight features of ICAM services that are particularly important. For instance, "Least Privilege" is a foundational principle of cybersecurity and is implemented in Zero Trust. In the context of cloud, where there is no well-defined perimeter, assigning user accounts and processes with specific, limited privileges is essential. As we elaborate on the CDM IDAM services in cloud, we

[3] Department of Homeland Security. "Cloud Requirements Catalog," Draft Version 1.0, December 2021.

will highlight ICAM considerations explored in the CDM cloud guidance documents, such as centralizing Identity Management.[4]

4.3 CDM FUNCTIONS RELATED TO IDAM REFERENCE ARCHITECTURE

The CDM capabilities and sub-capabilities defined in Table 4-2 are also included in the shaded section of Table 4-1 and are applicable to the IDAM reference architecture.

Table 4-2: CDM IDAM Capabilities and Sub-Capabilities

CDM IDAM Capabilities	Description
Manage Trust in People Granted Access (TRUST)	TRUST monitors vetted trust level and identifies *instances in which an authorized user does not comply with agency policy on TRUST*.
Manage Security-Related Behavior (BEHAVE)	BEHAVE ensures authorized users exhibit the appropriate behavior for their roles and identifies *instances in which an authorized user does not comply with agency policy on training, user agreements, or other agency-defined requirements*.
Manage Credentials and Authentication (CRED)	CRED ensures account credentials are assigned to, and only used by, authorized users or services and identifies *instances in which an authorized user's credentials do not comply with agency policy*.
Mobile Identity Management (MIM)	A sub-capability under CRED, MIM enables an agency to secure the use of mobile devices by provisioning a derived personal identity verification (PIV-D) credential.
Privilege Management (PRIV)	PRIV provides the agency with insight into risks associated with *authorized users not complying with related agency policy or being granted excessive privileges* to systems and information at any level of sensitivity.
Privileged Access Management (PAM)	A sub-capability under PRIV, PAM provides a PEP for privileged user Access Management, primarily for administrators. PAM also protects agency systems and networks by allowing only authorized user access as a privileged user and monitors their activities.
Identity Lifecycle Management (ILM)	A sub-capability under PRIV, ILM adjusts information in connected repositories to address changing privileged user positions and responsibilities, through adding and removing entitlements to systems, roles, and accounts based on agency rules. This will also prompt review of users' attributes to identify additional training and remove excess or unnecessary privileges.

Figure 4-3 shows a decomposition of the IDAM capability area. TRUST, BEHAVE, CRED, and PRIV[5] each have the following functions:

- Establish agency-desired state in machine-readable policies; captures agency policy and desired-state information in machine-readable form.
- Collect information from authoritative sources; collects actual-state information from authoritative sources, which are existing systems that vary by agency.
- Compare agency's actual state to policy; compares agency-desired state with collected actual state and identifies defects.
- Display information and generate reports locally; provides for information to be displayed locally on a tool, sent to a printer, or output to a document.
- Report information to the Agency Dashboard; reports actual-state information and defects to the Agency Dashboard.

In addition, PRIV offers the ILM and PAM sub-capabilities for managing privileged user accounts and authenticating and authorizing privileged users, respectively. CRED has a MIM sub-capability for provisioning PIV-D credentials on mobile devices.

[4] Department of Homeland Security. "Continuous Diagnostics and Mitigation (CDM) Program Cloud Guidance Document, Volume 1, Architecture, Data Flows, and Data Sources," Version 2.0. Section 3.2.5. May 2020.
[5] Ibid.Table 1

ILM functions are as follows:

- ILM-1. **Manage workflow of user access permissions** function notifies the administrators and reviewers when changes to user accesses have been made, or require approval, and enforces approval policy.
- ILM-2. **Provision user accounts and entitlements** function provisions in-scope privileged user accounts and entitlements, providing users only the privileges necessary to perform their specific role within the agency.
- ILM-3. **Establish agency ILM-desired state in machine-readable policies** function captures the policies needed for ILM functionality, derived from agency policies.[6]

PAM functions are as follows:

- PAM-1. **Authenticate user access** function authenticates in-scope privileged users for access to target devices.
- PAM-2. **Authorize user access** function provides privileged users access to agency-defined target devices.
- PAM-3. **Validate PRIV accounts** function determines whether all active and inactive privileged user accounts are correctly identified within the agency.
- PAM-4. **Establish agency PAM desired state in machine-readable policies** function captures the policies that address access to protected resources.[7]

The single MIM function is as follows:

- MIM-1. **Provision the PIV-D credential** function authenticates the user associated with the device with the user's PIV card for proof of user's identity.[8] This binds the user's identity with the DPC and provisions the credential on the mobile device.

[6] Department of Homeland Security. "Continuous Diagnostics and Mitigation (CDM) Program Cloud Guidance Document, Volume 1, Architecture, Data Flows, and Data Sources," Version 2.0, Sections 3.2.3, 3.2.4, 3.2.5, and 3.2.8, May 2020.
[7] *Ibid,* 3.2.3, 3.2.12, and 3.2.13.
[8] There may need to be some support for special devices that have to be shared (e.g., Emergency Medical Services devices across shifts).

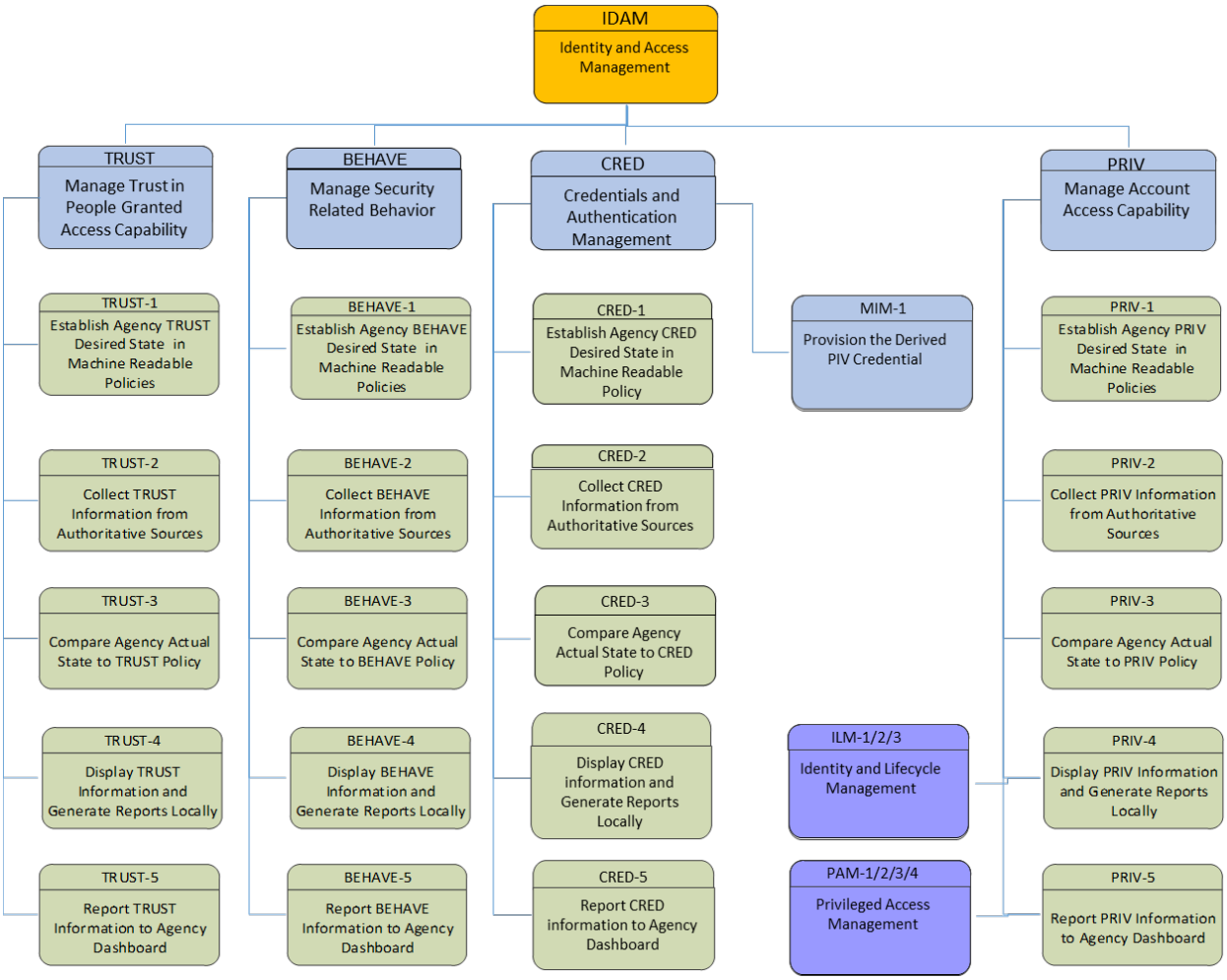


Figure 4-3: IDAM Capability Area Functional Hierarchy

Initially, CDM IDAM capabilities were delivered via three task orders:

- CREDMGMT – Established a Master User Record (MUR) [Identity Governance and Administration (IGA)] for unprivileged users and collection and evaluation of TRUST, CRED, and BEHAVE attributes for Chief Financial Officers (CFO) Act of 1990 agencies.
- PRIVMGMT – Established MUR for privileged user and the collection and evaluation of TRUST, CRED, BEHAVE, and PRIV attributes for CFO Act agencies and select non-CFO Act agencies.
- DEFEND – Fulfilled the MUR across the users and services and additional capabilities for targeted agencies for ILM and PAM sub-capabilities for CFO Act agencies.

Figure 4-4 provides an overview of the CDM IDAM capability area. TRUST, BEHAVE, CRED, and PRIV collect and provide the data to the CDM MUR. PAM controls privileged access on target devices identified by the agency. ILM provides lifecycle management of accounts used in PAM.

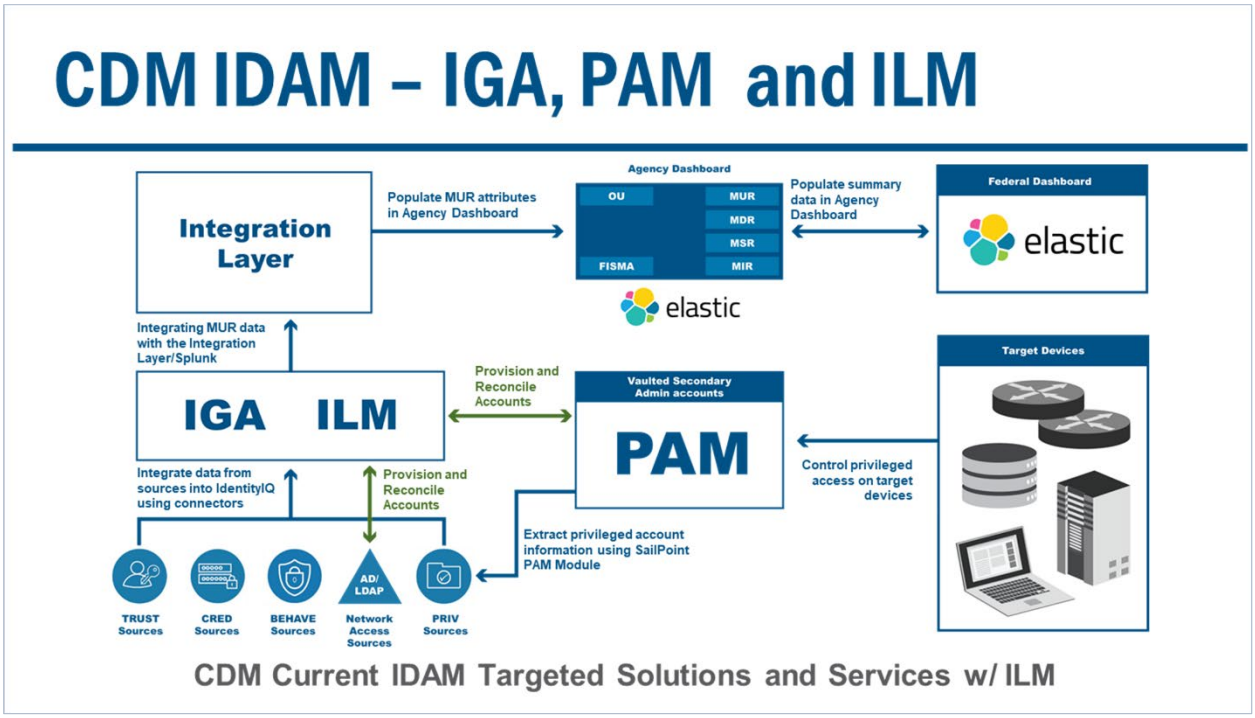


Figure 4-4: CDM Current IDAM Targeted Solutions and Services

Section 6 describes how these capabilities integrate with the FICAM reference architecture described in Section 5.

5. ARCHITECTURE CONCEPTS

This section provides an overview of a reference architecture into which CDM expects to incorporate processes and data when integrating at an agency. It also describes concepts such as cloud, Zero Trust, governance, and federation as applied to the ICAM community.

5.1 FICAM ARCHITECTURE

An overview of the FICAM architecture, a collaboration between the General Services Administration (GSA) and the Federal Chief Information Officer (CIO) Council,[9] is provided in this section and used in Section 6 to develop the CDM ICAM reference architecture, which shows how CDM integrates with FICAM. Per the FICAM architecture:

"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."

Figure 5-1[10] shows the FICAM practice areas and provides a brief description of each.

[9] General Services Administration, "The Federal Identity, Credential, and Access Management Architecture," Version 3.1, FINAL, January 6, 2021, accessed May 20, 2022, https://playbooks.idmanagement.gov/docs/ficam-arch.pdf.
[10] Ibid.

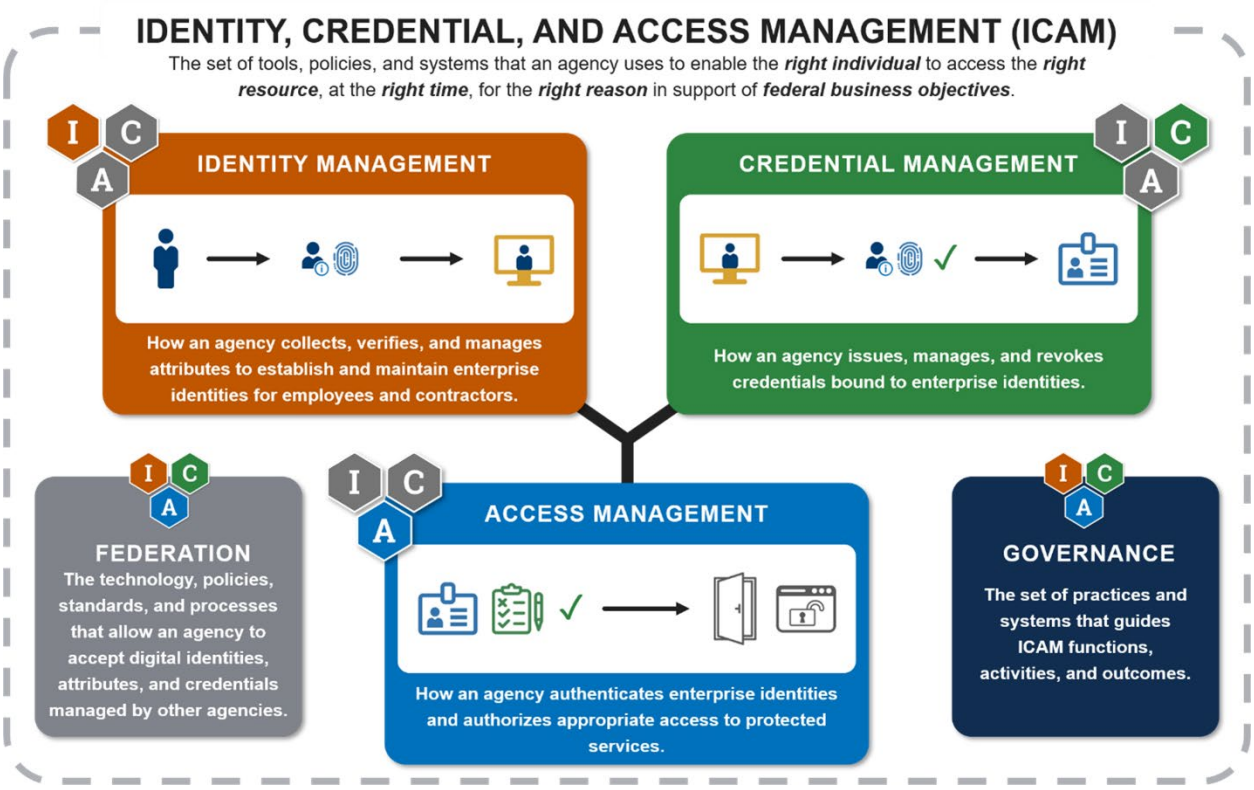


Figure 5-1: ICAM Practice Areas and Supporting Elements

The FICAM architecture services within each practice area and supporting element are shown in Figure 5-2[11] with brief descriptions.

[11] General Services Administration, "The Federal Identity, Credential, and Access Management Architecture," Version 3.1, FINAL, January 6, 2021, accessed May 20, 2022, https://playbooks.idmanagement.gov/docs/ficam-arch.pdf.

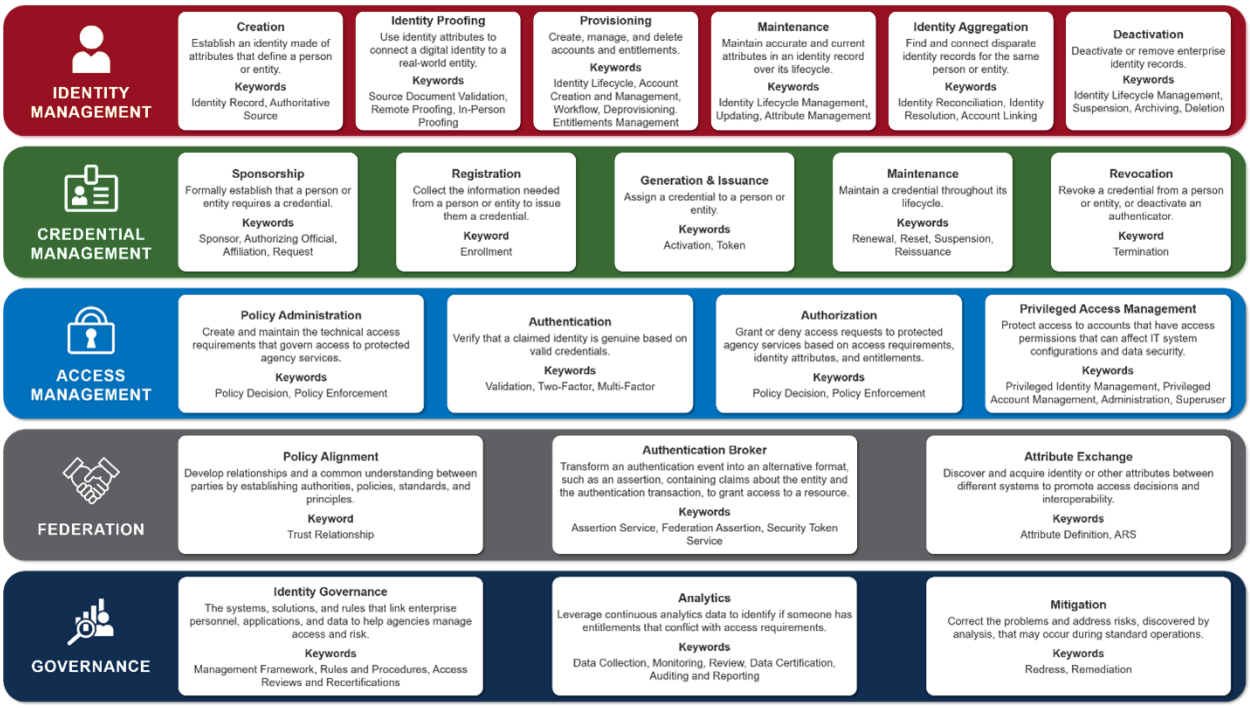


Figure 5-2: FICAM Services

5.2 CLOUD AND HYBRID COMPUTING MODEL

This section describes cloud computing as applied to the ICAM community. The cloud and hybrid computing model is well supported by the FICAM architecture.

Cloud computing is an evolving paradigm. The National Institute of Standards and Technology (NIST) definition in NIST SP 800-145 characterizes important aspects of cloud computing and is intended to serve as a means for broad comparisons of cloud services and deployment strategies and to provide a baseline for discussion of what cloud computing is and how best to use cloud computing. NIST presents a Deployment and Service Model.

The cloud deployment model is hardware oriented and is generalized by whoever owns the hardware:

- **Private Cloud**, where the user's organization owns the hardware.
- **Community Cloud**, where a set of organizations share the hardware.
- **Public Cloud**, where the hardware is owned by a Cloud Service Provider (CSP) and is shared with people outside the organization, in many cases the public. There are also hybrid versions. (For detailed definitions, see NIST SP 800-145.)

The cloud service model is an abstraction layer above the physical layer and is generated independently of hardware. NIST SP 800-145 defines three "As a Service" models:

- **Software as a Service (SaaS)**. The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure.
- **Platform as a Service (PaaS)**. The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or -acquired applications.

- **Infrastructure as a Service (IaaS).** The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources. (For detailed definitions, see NIST SP 800-145.)

Table 5-1, modified from the draft CDM Cloud Requirements Catalog, provides additional detail on the cloud service models and also offers ICAM-specific implications in the third column.

Table 5-1: Cloud Service Models and ICAM Implications

Cloud Service	Description	ICAM Implications
IaaS	IaaS provides the basic building blocks for IT. In an enterprise, these devices are typically routers, computers, servers, and storage centers. In the cloud, while the components may look a little different, the basics are the same. In the cloud, they are typically compute nodes, virtual private cloud, and large-scale data storage frameworks. IaaS provides the most flexibility over management, control, and configurations for a tenant.	The ICAM capability for IaaS will include access control solutions to protect the tenant's virtual infrastructure and to allow the tenant to manage access to all systems, software services, applications, and data assets within the virtual infrastructure.
PaaS	PaaS removes the need for organizations to manage the underlying virtual infrastructure, networking, and storage. These platforms enable organizations to rapidly develop solutions without the constraints of more specified platforms. Organizations have fewer concerns about management and procurement of hardware and software and can focus more on development.	The ICAM capability for PaaS includes access control solutions, allowing the tenant to use these features to protect the tenant's service platform and to administer access control policies for all applications and data assets hosted on the platform.
SaaS	SaaS provides a completed product that is run and managed by the CSP. With a SaaS offering, organizations do not have to think about how the service is maintained or how the underlying infrastructure is managed. Organizations only need to think about how they will use that piece of software.	ICAM capability for SaaS typically integrates with an existing agency ICAM solution and will develop and configure an access control method with policies for users and devices to protect the agency's application data hosted in the SaaS environment.

The traditional perimeter-centric ICAM architecture is shown in Figure 5-3. This legacy architecture is Active Directory (AD)-centric, leveraging that tool as the main service of user management, authentication, access, and authorization. There are some issues with the tool, including that AD may not be synchronized among the different capabilities, and agencies may misconfigure these services and need manual provisioning when updating ICAM capabilities. This manual configuration is labor-intensive, inefficient, and prone to errors. Additionally, AD has proven vulnerable to attacks involving privilege escalation and password and hash compromise.

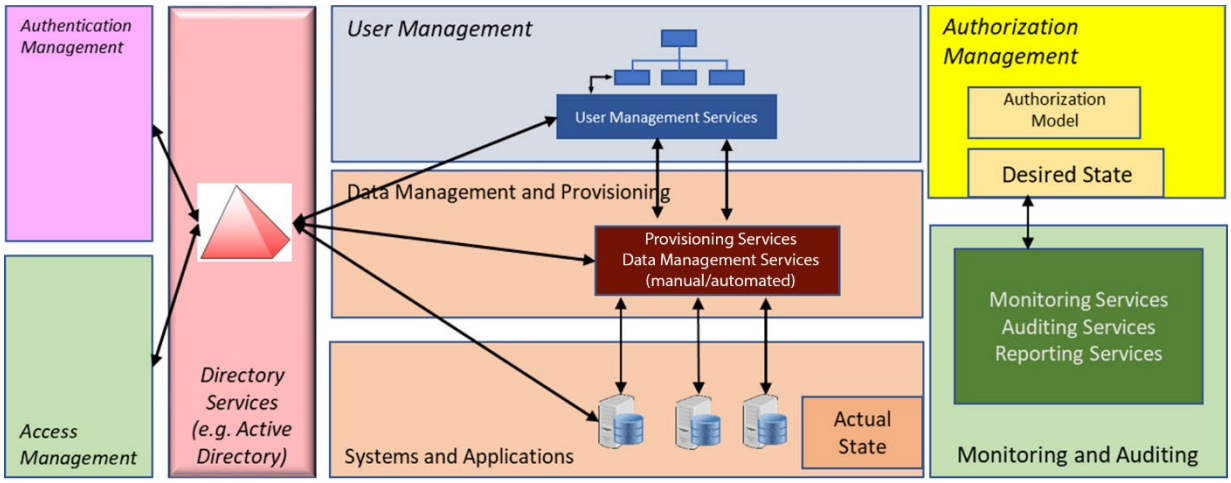


Figure 5-3: On-Premises ICAM Enterprise Architecture Model

The adoption of cloud services from a CSP impacts the methodologies, management, and responsibilities for ICAM. Protection shifts from on-premises infrastructure and data ownership to off-premises and hybrid custodial management. Figure 5-4 provides an overview of the relevant ICAM capabilities when users interact with cloud services and shows where CDM interacts.

Tools such as enterprise Cloud Access Security Broker (CASB)[12] and virtual directory service can be configured to support the attribute exchange service. When incorporated with the enterprise risk management capabilities, CASB can support risk-adaptive access policies for cloud Access Management. Agencies will decide whether to leverage existing on-premises privileged accounts for cloud applications or to create local cloud privileged accounts. Systems and applications are used to perform cloud functions. Authentication brokers and policy alignments are used to ensure an accurate access policy (which may include conditional access) for users and their organizations. CASB functionality is evolving, but it is expected that the functionality would support BOUND.

[12] Cybersecurity and Infrastructure Agency, "Trusted Internet Connections 3.0", Version 1.0, June 2022, https://www.cisa.gov/sites/default/files/publications/CISA%20TIC%203.0%20Cloud%20Use%20Case%20Draft_1.pdf.

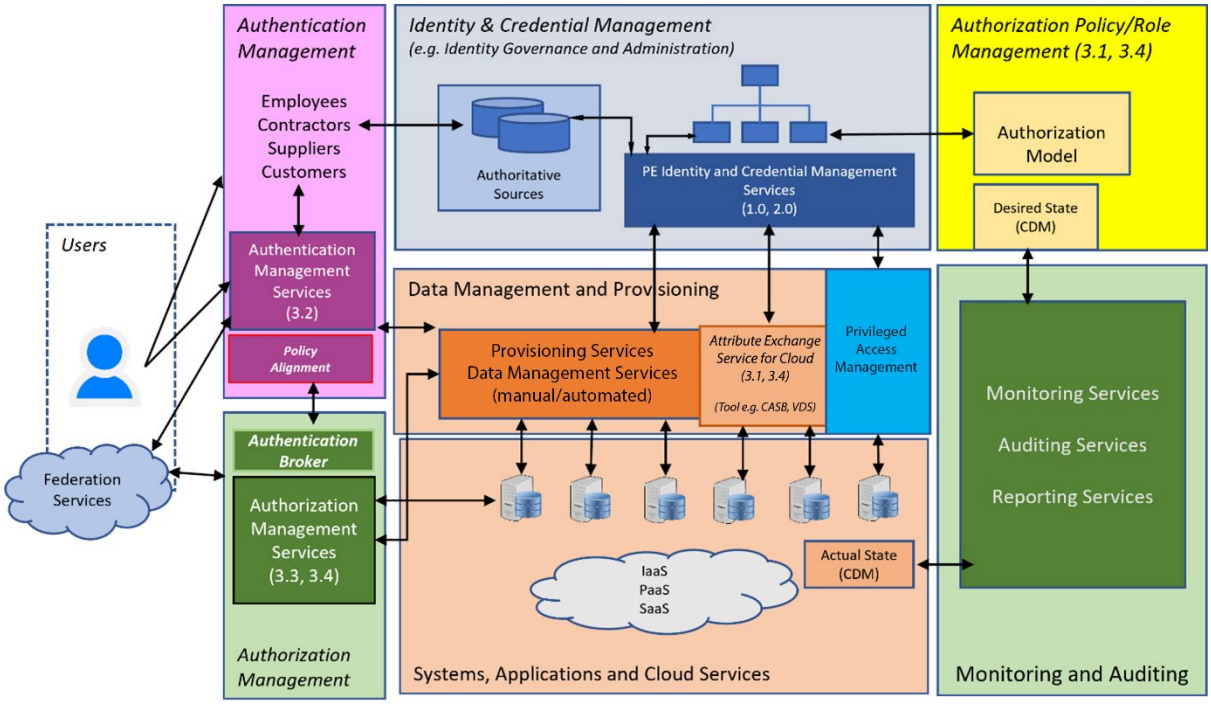


Figure 5-4: ICAM in Cloud Services Overview

CASB (represented in Figure 5-4 as a cloud tool within the Data Management and Provisioning capability) provides an interface to ensure consistent security policy between an enterprise and a CSP. CASB supports IaaS, PaaS, and SaaS cloud environments, and its detection capabilities can be out-of-band or in-line and include malware scanning via signatures and use of sandboxing. CASB also includes User and Entity[13] Behavior Analytics, which provides detection of anomalous behavior, based on rulesets of expected patterns such as an extremely high volume of file downloads on a user account. CASB protection capabilities can block malware when it is either uploaded to or downloaded from the cloud. CASB also includes Adaptive Access Control, a form of risk-adaptive access policy for cloud, which can block or limit access or provide step-up user authentication. Related to CDM, CASB generates logging information related to cloud policy conformance, and may also be able to serve as a means to pass HWAM or SWAM reporting data from the cloud; both of these may be relevant metrics for the CDM dashboard.[14] CASB functionality is adapting over time, but it is expected that CASB would support BOUND now and in the future. CASB is discussed in further detail in the CDM Cloud Guidance Document Volume 2, Section 5.1.

In Figure 5-4, blocks with numbers (e.g., 1.0, 2.0, 3.1) indicate the linkage between ICAM functions found in the CDM ICAM reference architecture (see Identity Management, Credential Management, and Access Management in Figure 5-5).

[13] Note that the term "entity" is used in this context to convey an NPE.
[14] Department of Homeland Security, "Continuous Diagnostics and Mitigation (CDM) Program Cloud Guidance Document, Volume 2, Cloud-Service Support for CDM," Version 2.0, May 2020.

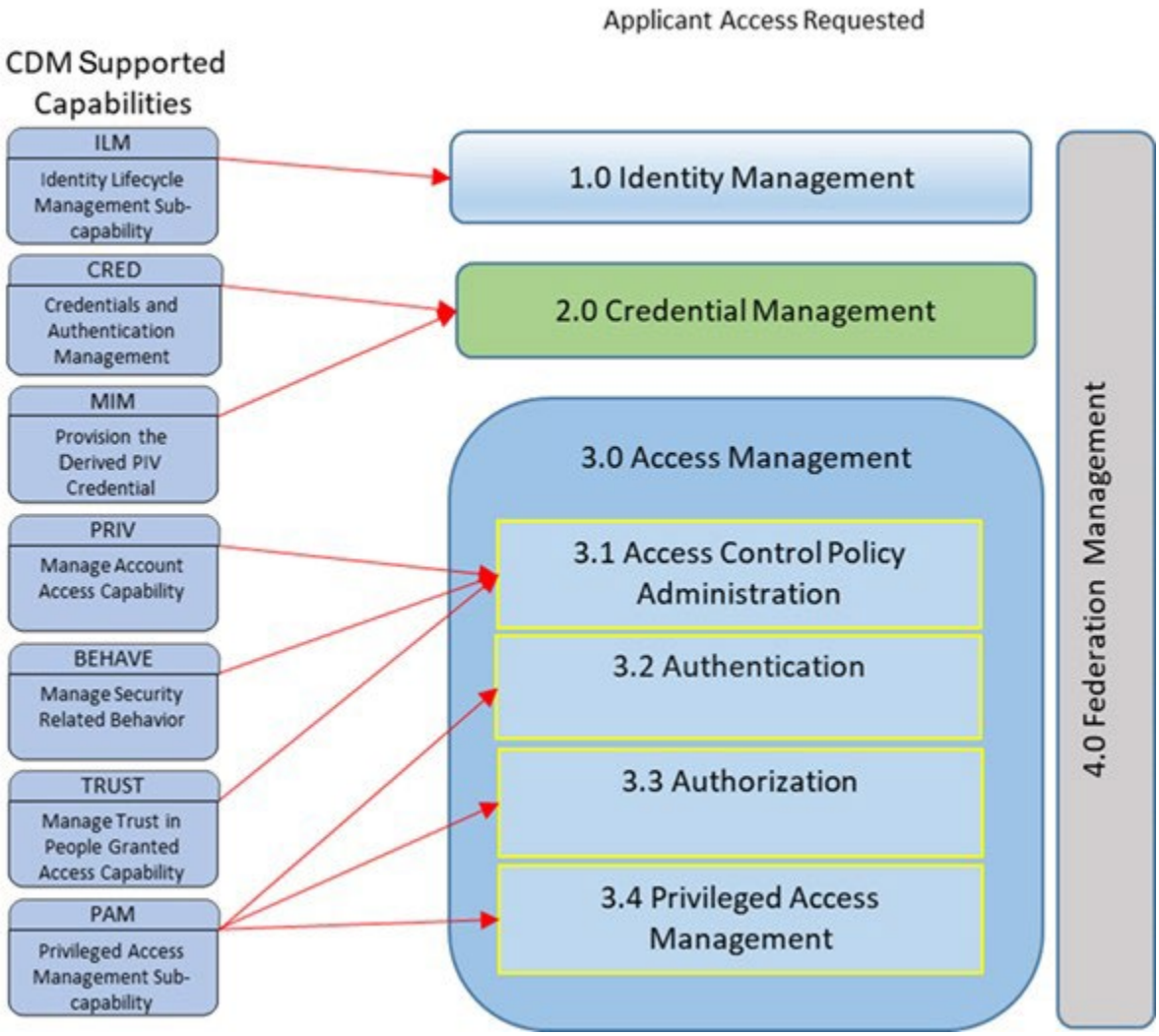
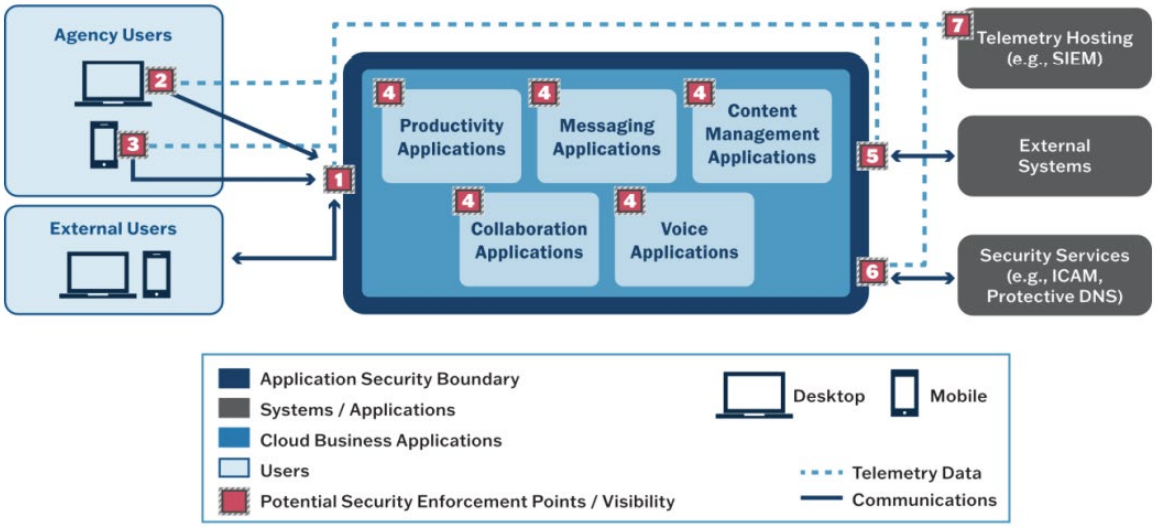


Figure 5-5: Top-Level CDM ICAM Functional Block Diagram

For cloud environments, CISA has developed a "Secure Cloud Business Applications (SCuBA) Technical Reference Architecture (TRA)." Figure 5-6 illustrates the security and visibility points for SCuBA. ICAM maps to Security Enforcement Point/Visibility (point 6 indicated in the figure). The TRA states, "Additionally, from a ZT [Zero Trust] perspective, while the security of these applications intersects with each of the pillars described in the ZT Maturity Model, the application security boundary most closely aligns with the application workload pillar."[15]

[15] Cybersecurity and Infrastructure Security Agency, "Secure Cloud Business Applications (SCuBA) Technical Reference Architecture (TRA)," April 2022, Request for Comment Draft, accessed July 25, 2023, https://www.cisa.gov/sites/default/files/2023-06/CSSO-SCUBA-TRA-guidance%20documentV2_508c.pdf



DNS: Domain Name System; SIEM: Security Information and Event Management

Figure 5-6: SCuBA Security and Visibility View

5.3 ZERO TRUST MODEL

This section describes Zero Trust as applied to the ICAM community. Zero Trust is a security model for a network architecture that trusts no device or user by default and authenticates every transaction. NIST released ZTA guidance[16] in 2020, promoting the adoption of Zero Trust for more robust network security. On May 12, 2021, President Biden issued EO 14028, calling for the federal government to adopt security best practices and advance toward implementing ZTA.[17] ICAM is essential to this adoption, as robust identity processes form the foundation of any ZTA. The cloud and hybrid computing model is well supported by the FICAM Architecture, although CISA believes the architecture features will be applied in increasing granularity across the ZTA.

The CISA Zero Trust Maturity Model v1.0 refers to the definition of Zero Trust in NIST SP 800-207: "a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised."

One of the Zero Trust guiding principles is to "treat every user, device, application/workload, and data flow as untrusted. Authenticate and explicitly authorize each to the least privilege required using dynamic security policies."[18]

The NIST SP 1800-35 series, "Implementing a Zero Trust Architecture" summarizes how the National Cybersecurity Center of Excellence and its collaborators are using commercially available technology to build interoperable, open standards-based ZTA implementations that align to the concepts and principles in NIST SP 800-207.

---

[16] National Institute of Standards and Technology (NIST), "Zero Trust Architecture, NIST SP 800-207," August 2020, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf.
[17] Executive Order 14028, "Improving the Nation's Cybersecurity," May 12, 2021, accessed July 25, 2023, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity.
[18] National Security Agency, "Embracing a Zero Trust Security Model," Version 1.0, February 2021, https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UO0115131-21.PDF.

This series comprises five volumes:

- NIST SP 1800-35A: Executive Summary
- NIST SP 1800-35B: Approach, Architecture and Security Characteristics
- NIST SP 1800-35C How-To Guides
- NIST SP 1800-35D: Functional Demonstrations
- NIST SP 1800-35E: Risk and Compliance Management

Figure 5-7 depicts the logical architecture of a general ZTA reference design independent of deployment models described in NIST SP 1800-35B.[19] It consists of three types of core components: policy engines (PEs), policy administrators (PAs), and policy enforcement points (PEPs). It also consists of several supporting components that assist the policy engine in making its decisions by providing data and policy rules related to areas such as ICAM, endpoint detection and response (EDR), endpoint protection platform (EPP), security analytics, and data security.

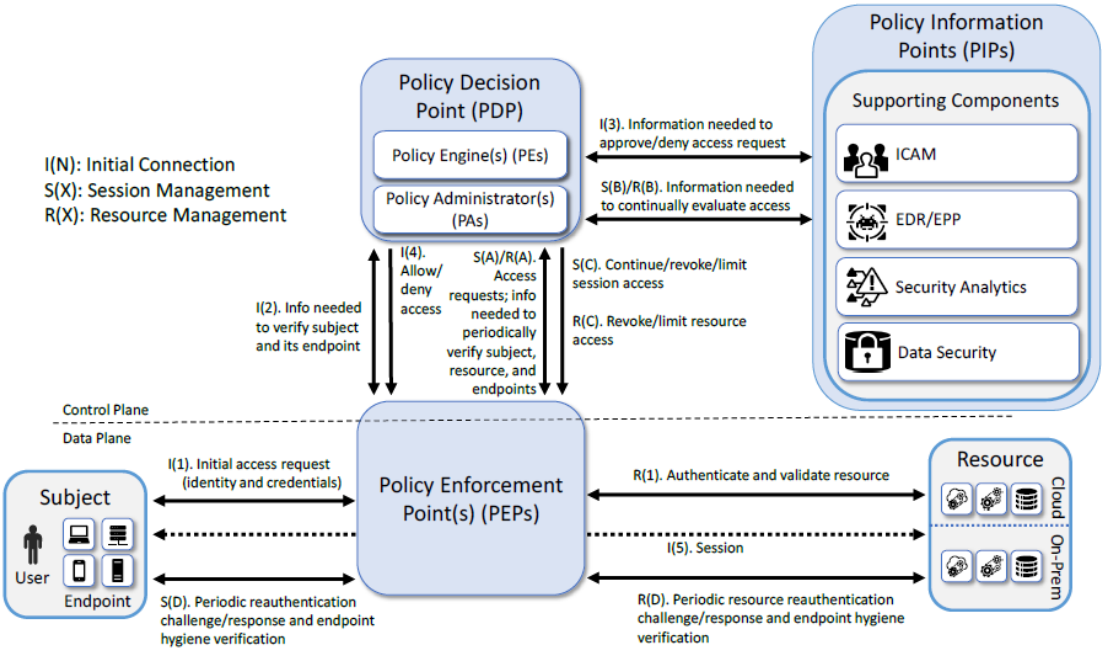


Figure 5-7: General Zero Trust Architecture (From NIST SP 1800-35B)

The various sets of information either generated via policy or collected by the supporting components and used as input to ZTA policy decisions are referred to as policy information points (PIPs). Each of these logical components may not directly correlate to a single architectural component. Some ZTA logical component functions may be performed by multiple software components, or a single software component may perform multiple functions.

Subjects (devices, end users, applications, servers, and other non-human entities that request information from resources) request and receive access to enterprise resources via the ZTA. Human subjects (i.e., users) are authenticated. Non-human subjects are both authenticated and protected by endpoint security. Enterprise resources may be located on premises or in the cloud. Existing enterprise subjects and resources are not part of the reference architecture itself; however, any changes required to existing endpoints, such as installing ZTA agents, should be considered part of the reference architecture.

[19] National Institute of Standards and Technology (NIST), "Implementing a Zero Trust Architecture Volume B: Approach, Architecture, and Security Characteristics, NIST SP 1800-35B" (Second Preliminary Draft), December 21, 2022, https://www.nccoe.nist.gov/sites/default/files/2022-12/zta-nist-sp-1800-35b-preliminary-draft-2.pdf.

Key ICAM components for implementing a ZTA include:[20]

- PEs and NPEs: Authenticate all users before providing access. Managing identities and providing secure multifactor authentication (MFA) credentials is the first step in determining who is requesting access.
- Endpoints: In addition to authenticating users, Zero Trust requires authenticating and approving endpoints, such as workstations, mobile devices, or Internet of Things (IoT) devices.
- Data, assets, applications, and services: Definition and implementation of access policies is needed to implement the continuous evaluation aspect of Zero Trust.[21]

The following describes the importance of establishing a strong ICAM foundation before implementing Zero Trust:

- Zero Trust cannot be achieved without strong identity management and mature ICAM capabilities for NPEs.
- A strong foundation of ICAM governance provides a comprehensive set of access control policies and guidelines, setting the foundation for agencies to implement Zero Trust principles.

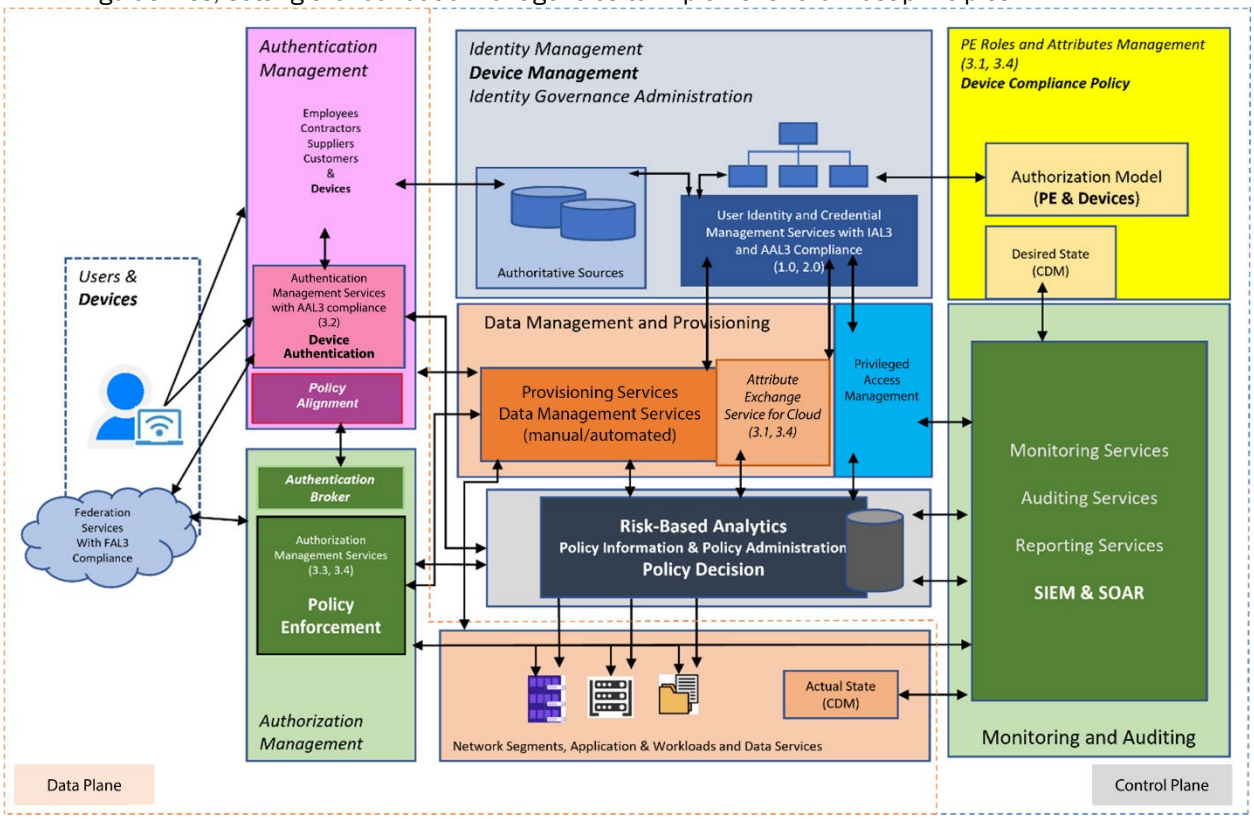


Figure 5-8: ICAM in Zero Trust Overview

[20] General Services Administration, "Identity, Credential, and Access Management Governance Framework Appendix C: ICAM and Zero Trust," Version 1.0, September 2021, accessed November 17, 2022, https://playbooks.idmanagement.gov/docs/playbook-identity-governance-framework.pdf.
[21] National Security Agency, "Embracing a Zero Trust Security Model," Version 1.0, February 2021, https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UO0115131-21.PDF.

Figure 5-9 depicts the foundation of Zero Trust, which is provided from the CISA Zero Trust Maturity Model.[22] The five pillars necessary to support Zero Trust are Identity, Device, Network/Environment, Application Workload, and Data. Each pillar helps plan, assess, and maintain the investments needed to progress toward a ZTA. Each of the five pillars includes general details regarding visibility and analytics, automation and orchestration, and governance for that pillar.

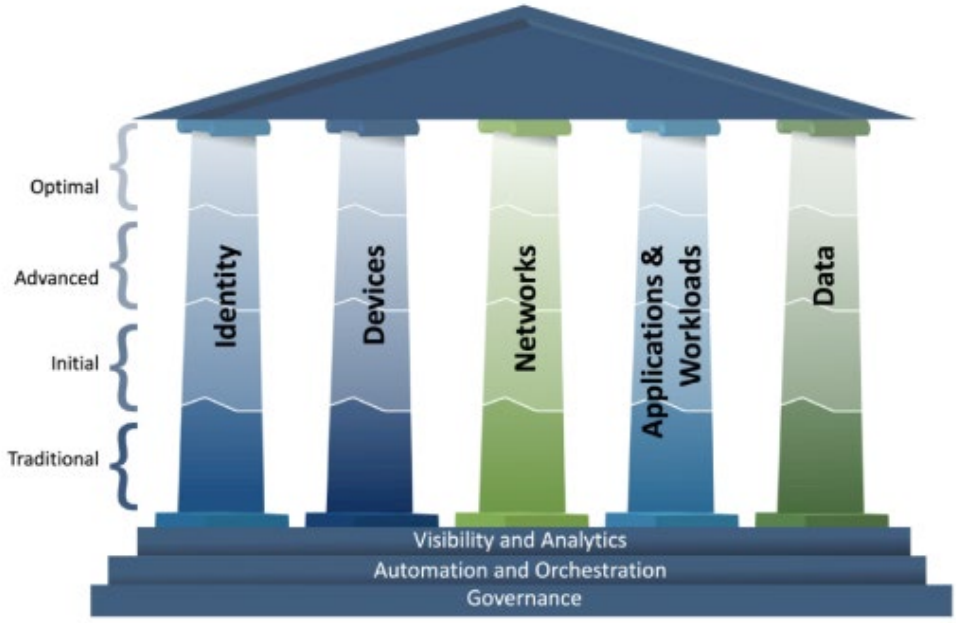


Figure 5-9: Zero Trust Maturity Evolution

5.4 FICAM REFERENCES FOR IDENTITY MANAGEMENT AND IDENTITY PILLAR

This section describes Identity Management as referenced in FICAM documents.

5.4.1 Identity Lifecycle Management Playbook

The FICAM Architecture's "Identity Lifecycle Management Playbook"[23] helps agencies understand how to shift the focus from managing the lifecycle of credentials to the lifecycle of identities as outlined in Section III of Office of Management and Budget (OMB) Memo 19-17 "Enabling Mission Delivery through Improved Identity, Credential, and Access Management."[24]

[22] Cybersecurity and Infrastructure Security Agency, "Zero Trust Maturity Model," Version 2.0, April 2023, accessed July 25, 2023, https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf.
[23] General Services Administration, "Identity Lifecycle Management Playbook," Version 1.2, December 15, 2022, https://playbooks.idmanagement.gov/playbooks/ilm/.
[24] Executive Office of the President, Office of Management and Budget. "Enabling Mission Delivery through Improved Identity, Credential, and Access Management," OMB-M-19-17, May 21, 2019, accessed May 20, 2002, https://www.whitehouse.gov/wp-content/uploads/2019/05/M-19-17.pdf.

5.4.2 Identity Management Cloud Playbook

The FICAM Architecture's "Cloud Identity Playbook"[25] describes a four-step playbook for the use of workforce ICAM services delivered in the cloud. Functions identified in the Identity Management section are:

- Automate identity (automate manual processes)
- Ensure accurate directory information
- Consider using a virtual directory
- Implement role-based entitlement management
- Employ NPE Identity Management

5.4.3 Digital Worker Identity Playbook

A digital worker is an automated, software-based tool, application, or agent that performs a task or process similar to a human user and uses artificial intelligence (AI) or other autonomous decision-making capabilities. Common types of digital workers include AI systems, Chatbot software tools, and machine learning processes.

NPE encompasses all entities with a digital identity, including organizations, hardware devices, software applications, and information artifacts. A subset of NPE, Digital Worker (DW) is an automated, software-based tool, application, or agent that performs a business task or process similar to a human user and uses Artificial Intelligence (AI) or other autonomous decision-making capabilities.[26]

Overall digital worker Identity Management process comprises three main steps (i.e., determine the impact, create an identity, and provide an identity) as described in the General Services Administration (GSA) digital identity worker playbook (Figure 5-10)[27].

Figure 5-10: Digital Worker Identity Management Process

The agency should use appropriate enterprise risk management capability and ICAM principles to assess the potential risks associated with the digital worker. An agency should be fully aware of its overall adverse impact level and assign a sponsor and custodian to the digital worker as part of its identity record while creating the digital worker's identity. The digital worker identity record should include data elements that support the digital worker identity lifecycle and operational processes and objectives, including data elements for identity catalog and monitoring.

5.5 CREDENTIAL MANAGEMENT

This section describes credential management as utilized by NPE, cloud, and Zero Trust.

[25] General Services Administration, "Cloud Identity Playbook," Version 1.0, January 20, 2022, accessed May 20, 2022, https://playbooks.idmanagement.gov/playbooks/cloud/.
[26] General Services Administration, "Digital Worker Identity Playbook," Version 1.1, January 5, 2021, accessed December 8, 2022, https://playbooks.idmanagement.gov/playbooks/dw/.
[27] Ibid

5.5.1 Credential Management Cloud Concepts

The GSA's "Cloud Identity Playbook" [28] digital identity concepts for Credential Management are:

- Allow multiple phishing-resistant authenticators. Consider a secondary authenticator option beyond a PIV card.
- Perform risk assessments on NPE credentialing.
- Memorize secrets. Consider MFA and phishing-resistant authenticators.

5.6 ACCESS MANAGEMENT

This section describes access management as utilized by NPE, cloud, and Zero Trust.

5.6.1 Access Management Cloud Playbook

The GSA's "Enterprise Single Sign-On (SSO) Playbook"[29] digital identity concepts for Access Management include :

- SSO is a component of ICAM that agencies use to centralize access to applications.
- SSO enables end users to log into multiple applications using extensible MFA options.
- SSO extends capabilities for applications that do not natively support MFA.
- SSO provides a centralized access point to onboard cloud applications.

5.6.2 Secure Cloud Business Applications IDaaS Guidance

CISA's "Secure Cloud Business Applications (SCuBA) Technical Reference Architecture (TRA)" states, "An alternative architecture that is becoming more prevalent for agencies leverages a cloud-based Identity as a Service (IDaaS) provider for authentication directly in the cloud (e.g., using a PIV-based credential). Such an architecture adopts a shared responsibility model in which the IDaaS provider assumes responsibility for security of key components of the platform (e.g., cryptographic material required for federation protocols) while the agency remains responsible for secure configuration. Some responsibilities, such as monitoring for threats, are shared between the agency, the vendor, and CISA in this model."[30]

CISA's "Secure Cloud Business Applications (SCuBA) Technical Reference Architecture (TRA)" mentions that some parts of access management are configured specifically within the cloud business applications. It states, "ICAM is critical to securing a cloud application. Many parts of ICAM should be managed enterprise-wide (identity lifecycle, issuance of root credentials, and privilege role assignment, etc.). However, some parts of access management are configured specifically within the cloud business applications. This is especially true with respect to managing end-user access. One important aspect is strong administrative controls and least privilege. Policies—such as Conditional Access in M365 or Context Aware Access in GWS [Google Workspace]—enable limiting access only to authorized and up-to-date devices. Such policies should be enabled to tie together the Secure Cloud Access and endpoint protection technologies. These policies 'close the loop' by ensuring that agency data is only accessible by devices that follow the agency's desired security posture."

[28] General Services Administration, "Cloud Identity Playbook," Version 1.0, January 20, 2022, accessed May 20, 2022, https://playbooks.idmanagement.gov/playbooks/cloud/.
[29] General Services Administration, "Enterprise Single Sign-On Playbook," Version 1.1, February 12, 2021, accessed December 8, 2022, https://playbooks.idmanagement.gov/playbooks/sso/.
[30] https://www.cisa.gov/scuba

5.7 FEDERATION

Federation is the technology, policies, standards, and processes that allow an agency to accept digital identities, attributes, and credentials managed by other agencies.[31]

Federation in the context of FICAM, external to single-agency federation, supports sharing and acceptance of digital identities, attributes, and credentials managed by other agencies, deploying standards such as OpenID Connect (OIDC) for the Identity layer and OAuth 2.0 for the Authorization layer. OIDC allows end-user verification of clients and applying this with OAuth 2.0 asserts attribute-based privileges. SSO uses these same assertion protocols to share and accept digital identities with Agencies and other Federal applications.

The use of Enterprise SSO is highly recommended because it limits the complexity and risks of direct credential enablement. With SSO-based Identity Federation, authentication transactions are standardized regardless of the credentials or authenticators, and user management activities can be consolidated under the Enterprise SSO.[32]

5.7.1 Federation Assumptions and Constraints

The following are assumptions and constraints to keep in mind:

- Agencies should ensure their federation services meet NIST SP 800-63C requirements.
- Agencies should establish the procedures and protocols by which security and identity attributes will be exchanged between Access Management control points and PDP for applications within their control that are used by other organizations.
- Members within the federation should publish and agree to the terms and conditions by which an entity can be granted access (authentication) and the extent of authorization.
- Agencies may contract out part or all of their externally facing Access Management capabilities by subscribing to an ICAM service being offered by another agency.
    - If the service being provided operates as an Authoritative Attribute Service (AAS), the relationship between the subscribing agency and the subscribed agency Service Provider should be made known to all members of the attribute federation. The Service Provider should ensure it is maintaining the confidentiality, integrity, and availability of those attributes as described in an attribute practice statement.

5.7.2 Federation Functions

The federation functions shown in Figure 5-7 from Access Management are described in the following subsections. For each function, a general description is provided, as well as CDM's support of that function, as applicable.

5.7.2.1 Authentication at the IDP

The Authentication function verifies the identity or other attributes claimed by or assumed of an entity. This function ensures only authorized entities with a valid set of attributes are granted access. It also validates the entity identity to ensure the identifier presented in the access request is valid. Functions must be implemented to ensure the form and validity of the mapping of the entity to its attributes. This function validates the entity attributes to ensure the attributes presented in the access request are valid or assumed. Functions must be implemented to ensure the form and validity of the attributes.

[31] General Services Administration. "The Federal Identity, Credential, and Access Management Architecture," Version 3.1, FINAL. January 6, 2021, accessed May 20, 2022. https://playbooks.idmanagement.gov/docs/ficam-arch.pdf.
[32] General Services Administration, "Enterprise Single Sign-On Playbook," Version 1.1, February 12, 2021, accessed December 8, 2022, https://playbooks.idmanagement.gov/playbooks/sso/.

Authentication consists of the following:

- Credential Validation: Ensures the integrity, provenance, and authority of the presented credential and that the credential is issued by a trusted authority and is not expired, revoked, voided, or tampered with.
- Factor Validation: Determines the strength of an identity claim by validating the factors 'something you know, have, and/or are.' Ensure the individual who was issued the credential is the same individual presenting it.
- Session Management: Enforces authentication and timeout policies for multiple entities concurrently accessing the infrastructure.
- Policy Alignment: Develops trust relationships between parties by establishing authorities, policies, standard communication protocols, and principles.[33]
- Authentication Broker: Transforms an authentication event into an alternative format, such as an assertion, containing claims or attributes about the entity and the authentication transaction, to grant access to a resource.[34]

5.7.2.2 Authorization is the Responsibility of the Relying Party (Service Provider)

The Authorization function grants access privileges to entities and provides for the mapping of information about entities and environmental context to an entity.

Authorization consists of the following:

- Policy Decision: Makes an access control decision based on access control policies (i.e., allow, deny, or allow with obligations).
- Policy Enforcement: Executes an access control decision based on the policies.
- Attribute Exchange: Discovers and shares identity attributes among different enterprise domains and cloud-hosted applications (for Federation).

5.7.3 Federation in the Cloud Identity Playbook

Federation plays a leading role in the delivery of cloud services and creating a Zero Trust architecture. The FICAM Architecture's Cloud Identity Playbook concepts for federation are: [35]

- Within the same trust domain, use the assertion profile.[36]
- Across agency domains, develop and use a federation trust framework that includes the following:
  - Governance
  - Technical and Security Requirements (Formats, Attributes, etc.)
  - Legal Agreements
  - Conformance Criteria – Federal Public Key Infrastructure (PKI) third-party audit
  - Recognition (Use of Federal PKI member resources)
  - IDaaS (See section 4.4.4.1) can support both federation and SSO

[33] General Services Administration, "The Federal Identity, Credential, and Access Management Architecture," Version 3.1, FINAL, January 6, 2021, accessed May 20, 2022, https://playbooks.idmanagement.gov/docs/ficam-arch.pdf.
[34] General Services Administration, "The Federal Identity, Credential, and Access Management Architecture," Version 3.1, FINAL, January 6, 2021, accessed May 20, 2022, https://playbooks.idmanagement.gov/docs/ficam-arch.pdf.
[35] General Services Administration, "Cloud Identity Playbook," Version 1.0, January 20, 2022, accessed May 20, 2022, https://playbooks.idmanagement.gov/playbooks/cloud/.
[36]The assertion profile can help to identify if and how each application might be able to support a given assertion protocol. This information is sent from an IdP to a relying party (such as the CSP).

5.8 ICAM GOVERNANCE FRAMEWORK

Governance is the set of practices and systems that guides ICAM functions, activities, and outcomes.[37] The FICAM Architecture's ICAM Governance Framework states that Program Governance and Leadership provides an organization framework to support ICAM Federation, and it includes a high-level framework for governance and leadership. This includes recommendations for a Program Governance Body, with defined roles and responsibilities, and a Component Governance team also needs to be established with the agency's ICAM-related program managers and IT experts. Topics also cover the need for a Program Management Office (PMO) in support of FICAM, which includes the establishment of PMO Roles and Responsibilities and a PMO Governance Structure.[38]

5.8.1 Governance Cloud Concepts

The GSA cloud playbook concepts for governance are:

- Certify access to application owner or manager.
- Plan for contingencies to verify IDaaS availability.
- Perform configuration monitoring for changes.
- Use policy-based governance.
- Monitor activity logging for all users.

5.8.2 CISA Zero Trust Governance Maturity

The CISA Zero Trust Maturity Model[39] shows governance as underpinning all pillars and foundation layers. For the Identity pillar, there is a recognized difference in maturity that agencies will undergo as they modernize and adopt a ZTA. Identity pillar maturity is described as:

- Traditional: Agency manually audits identities and permissions after initial provisioning using static technical enforcement of credential policies (e.g., complexity, reuse, length, clipping, and MFA).
- Advanced: Agency uses policy-based automated access revocation. There are no shared accounts.
- Optimal: Agency fully automates technical enforcement of policies. Agency updates policies to reflect new orchestration options.

6 CDM IMPLEMENTATION OF FEDERAL ICAM ARCHITECTURE

This section is organized by FICAM practice area. FICAM services are used as a basis for the functions developed to describe CDM's functionality in each of the practice areas. Figure 5-5 provides a top-level view of the FICAM practice areas and the related CDM functions (3.1 to 3.4 outlined in yellow).

- CDM CRED, PRIV, BEHAVE, and TRUST collect desired and actual states. The actual state shows the respective capabilities and comparing the desired state and actual state allows reporting of defects.
- CDM's ILM functionality in Identity Management is focused on the lifecycle management of privileged user identities.
- CDM's MIM capability is a sub-capability under CRED that can manage the PIV-D credential lifecycle, including issuance, credential renewal, reissuance, temporary activation and deactivation, and revocation and deletion through the EMM.

[37] General Services Administration, "The Federal Identity, Credential, and Access Management Architecture," Version 3.1, FINAL, January 6, 2021, accessed May 20, 2022, https://playbooks.idmanagement.gov/docs/ficam-arch.pdf.
[38] "FICAM Program Governance and Leadership," GSA, accessed August 10, 2023, https://playbooks.idmanagement.gov/pm/governance/.
[39] Cybersecurity and Infrastructure Security Agency, "Zero Trust Maturity Model," Version 2.0, April 2023, accessed July 25, 2023, https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf.

- PAM provides a PEP for privileged user Access Management. The key CDM operational ICAM functions that support the mapped FICAM services are PAM and ILM.

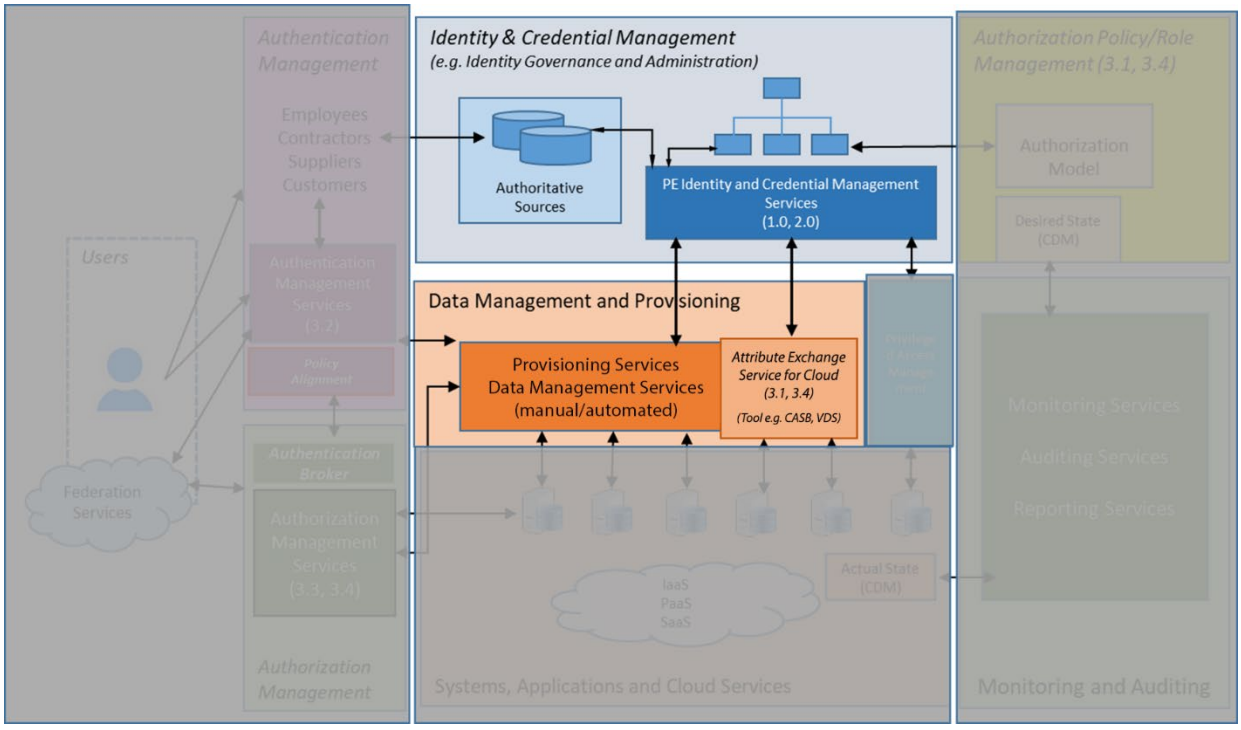
The following subsections describe the ICAM reference architecture and how CDM functionality supports the ICAM architecture through function description and some use cases. For each use case, we note whether an actor is described in FICAM, in CDM, or in both representations. This allows an observer to see where a CDM solution has contributed explicitly to FICAM services, has unique features described in CDM, and where there are gaps. Each section includes:

- A description of the FICAM practice area and related CDM capabilities
- Assumptions and constraints
- Functions
- Use cases that highlight the related CDM functionality
- Traceability between FICAM practice areas and related CDM capabilities

6.1 IDENTITY MANAGEMENT

Identity Management (Figure 6-1) is how an agency collects, verifies, and manages attributes to establish and maintain enterprise identities for Federal government employees, contractors, and authorized mission partners (i.e., PEs), and NPEs, which are services or systems accounts operating on behalf of an enterprise identity. In this context the service does not apply to public or consumer Identity Management,[40] rather to identities managed by the organization or agency.

A key theme in OMB Memo 19-17 is for federal agencies to shift the focus from managing the lifecycle of credentials to managing the lifecycle of identities as they evolve in an agency.



[40] General Services Administration. "The Federal Identity, Credential, and Access Management Architecture," Version 3.1, FINAL. January 6, 2021, accessed May 20, 2022. https://playbooks.idmanagement.gov/docs/ficam-arch.pdf.

Figure 6-1 ICAM in Identity Management

ILM is the evolution process of identity from creation to retirement. The lifecycle management process includes three distinct phases with individual steps in each phase.[41] These phases are known as the Joiner-Mover-Leaver process.

1. Phase 1 – Joiner

   There are three steps defined in phase 1. The first step is the creation of a new user identity record with attributes, roles, or group information that define a person or entity. The second step is a process to validate identity documentation from an authoritative data source to connect a digital identity to a real-world entity. This step is also known as Identity Proofing. The Identity Proofing process is part of the credential issuance process outside the agency Identity Management process. The third step is the identity provision, a process to manage identity attributes or account lifecycle.

2. Phase 2 – Mover

   There are two steps defined in phase 2. The first step is to maintain accurate and current attributes in an identity record over its lifecycle. The second step is to perform Identity Aggregation to connect disparate identity records for the same person or entity.

3. Phase 3 – Leaver

   Phase 3 is the process to deactivate or remove a MUR or identities associated with a MUR.

As part of the Enterprise Identity Management system, the Enterprise Directory Service often serves as the centralized repository to store and manage the identity records. This enterprise directory may reside in the cloud and require synchronization or virtualization of identity records and attributes from multiple sources. Examples of identity attributes are core identity attributes, authentication attributes, and entitlement attributes. The core identity attributes often include locally unique identifiers and characteristics that support identity resolution. The authentication attributes provide details that support identity claim resolution and identity binding that supports authentication. The entitlement attributes provide characteristics that support the resolution of access control policies.[42]

Identity Management, as shown in Figure 6-1, maps and maintains identifiers to verify PEs and NPEs so that both may be validated to gain access to controlled objects. The Identity Management function creates, provisions, manages, and archives globally unique identifiers throughout the lifecycle of the identity. Federal Information Processing Standard (FIPS) 201-3 states the minimum requirements for a federal PIV system that meets the control and security objectives of Homeland Security Presidential Directive (HSPD)-12, including Identity Proofing, registration, and issuance. FIPS 201-3 provides detailed technical specifications to support the control and security objectives of HSPD-12 as well as interoperability among federal departments and agencies.

In all cases, ILM relies on agency policy to guide the management of administrative provisioning and de-provisioning (for terminated or transferred users). Agency policy is also used through the establishment of desired state in machine-readable policies. This guides the workflow for privileged user access permissions, enabling notification when changes to user accesses have been made and when approval is required. ILM manages in-scope privileged user accounts and entitlements, providing users only the privileges necessary to perform their specific role within the agency.

[41] Idib.
[42] General Services Administration, "The Federal Identity, Credential, and Access Management Architecture," Version 3.1, FINAL, January 6, 2021, accessed May 20, 2022, https://playbooks.idmanagement.gov/docs/ficam-arch.pdf.

CDM Relationship to Identity Management: CDM has focused Identity Management functionality in two areas: providing Identity Governance and Administration (IGA) by instantiating a MUR, and through ILM functionality where CDM focuses on privileged users. CDM supports automatic provisioning of accounts for new hires with basic privileges because, in general, one must have an unprivileged account prior to gaining administrative privileges. Although CDM primarily focuses on human users that interactively log into agency systems, CDM has included NPEs in the CDM requirements to allow agencies that have sufficient maturity in managing human privileged users to expand to incorporate NPE in their PAM implementations.

6.1.1 Assumptions and Constraints

The following assumptions and constraints apply to Identity Management:

- It is assumed that agencies create human digital identities in accordance with FIPS 201-3, NIST SP 800-63A, NIST 800-157, and EO 13764.
- Human digital identities that are part of Access Federation should be created in accordance with NIST SP 800-63A and be assured at Identity Assurance Level (IAL) 2 or IAL3.
- Agencies should document their process describing the IAL associated with their digital identities.
- A given identity may have multiple responsibilities or duties, each of which may have entitlements associated with them. Entities, on the other hand, are assumed not to have multiple responsibilities, so there will not be multiple attributes associated with an entity.
- A digital identity is always unique in the context of a digital service but does not necessarily need to uniquely identify the subject in all contexts (see NIST SP 800-63).
- CDM manages agency NPEs within the PRIV and PAM capabilities.

6.1.2 Functions

The Identity Management functions shown in Figure 6-2 are described in the following subsections. For each function, a general description is provided, as well as CDM's support of that function, as applicable.

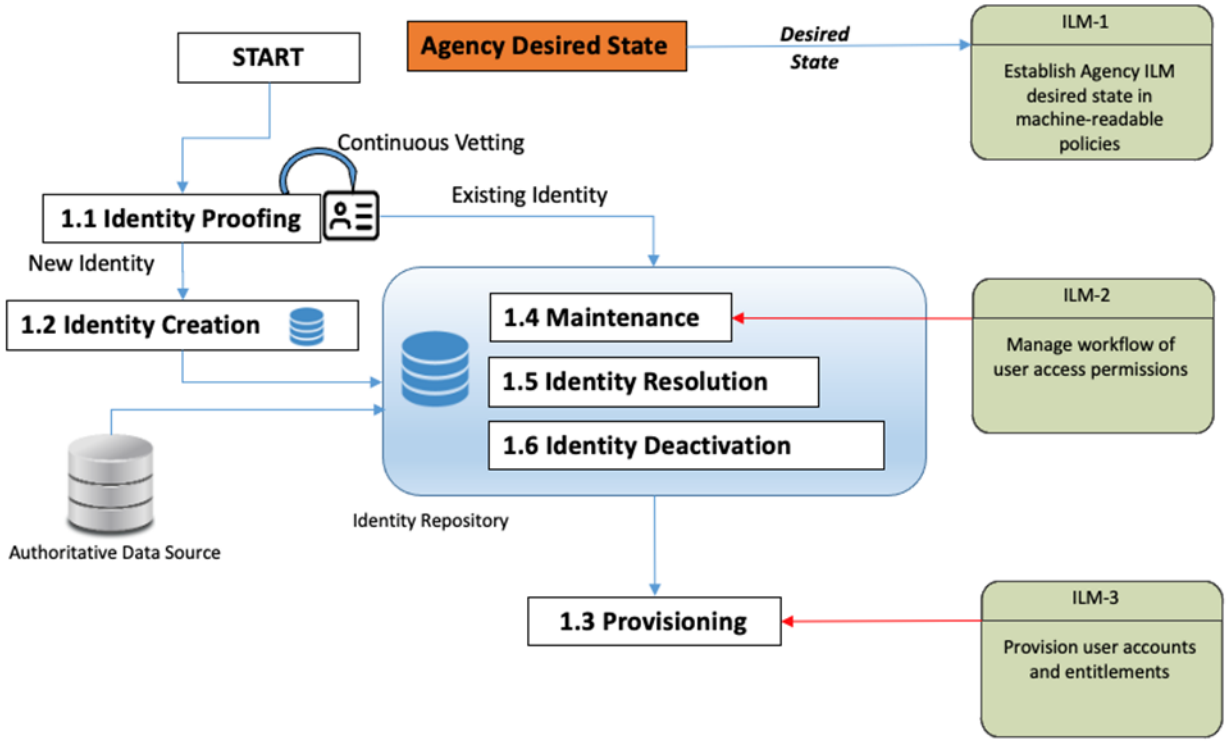


Figure 6-2: Identity Management Functional Block Diagram

6.1.2.1 Identity Creation

The Identity Creation function creates an identity record consisting of attributes that uniquely characterize and identify an entity. It contains a combination of identification attributes obtained from authorized sources as well as attributes created by the function. Entity identity records must contain at least one unique identifier that is used to represent a person's identity and associated attributes to distinguish that person's record from others. The unique identifier could be, for example, a first and last name, card number, or computer account identification.

CDM-Related Functionality: CDM assumes that agencies have accepted an employee and contractor to operate within their environment (usually through FIPS 201-3-related processes). CDM accepts that identity as valid when the elements of TRUST and CRED meet desired state. Identity is a prerequisite for the CDM ILM function.

6.1.2.2 Identity Proofing

The Identity Proofing function validates a requestor's identity information as a requirement for managing that identity. The requestor could be a PE making a request for themselves or an authorized party acting on behalf of an NPE or a different PE. Proofing decisions are based on sound criteria for verifying the entity's identity.

There are several standards that discuss proofing. HSPD-12 identifies information that shall be strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation; can be authenticated electronically; and is issued only by providers whose reliability has been established by an official accreditation process. NIST SP 800-63A addresses how PEs can prove their identities and become enrolled as valid subscribers within an identity system. It provides requirements for proofing identities and enrolling for one of three levels of risk mitigation in both remote and onsite scenarios.

CDM-Related Functionality: CDM assumes that agencies have accepted an employee or contractor to operate within their environment (usually through FIPS 201-related processes) and that Identity Proofing has been

concluded. CDM ensures this has occurred by accepting assertions of PIV issuance within the CRED capability and valid suitability via the CDM TRUST capability.

6.1.2.3 Identity Aggregation

The Identity Aggregation function merges, collects, links, and connects identity information from disparate identity information and access control profiles for the entity within the organization.

CDM-Related Functionality: The CDM MUR tool function provides Identity Aggregation when establishing and maintaining the user records from Agency Authoritative Sources.

6.1.2.4 Provisioning

The Provisioning function creates, manages, and deletes accounts and entitlements for application access control purposes for systems that rely on valid identity information. For example, the Provisioning function can propagate entity information to the AD server for access control and further distribution to remote workstations. Provisioning is performed after the Maintenance, Identity Aggregation, and Identity Deactivation functions to ensure the changes are pushed to the related systems.

CDM-Related Functionality: CDM ILM provides provisioning primarily for privileged users. CDM is primarily focused on the lifecycle of privileged users that can have impact on the infrastructure. The CDM ILM function supports the provision that for a user's privileged lifecycle to be managed, the user must first be an unprivileged user, and CDM can support that function.

6.1.2.5 Maintenance

The Maintenance function keeps identity attributes current in the identity record of an entity over its lifetime. Maintenance actions include updating personal attributes, organizational attributes, unique identifiers, entitlements, roles, and references to authoritative sources. Examples include name change, organization change, and changes to personally identifiable information (PII).

CDM-Related Functionality: CDM provides lifecycle management for users by enumerating authoritative source information and by providing account lifecycle for privileged user identities.

6.1.2.6 Identity Deactivation

The Identity Deactivation function can temporarily suspend, permanently deactivate, archive, or remove records, based on administrator action or per automatic policy (e.g., time expiration of credentials).

CDM-Related Functionality: CDM provides lifecycle management for privileged user identities. CDM supports review to include identifying IDAM information related to deactivated accounts. CDM can provide account deactivation through the ILM capabilities.

6.1.3 Use Cases

6.1.3.1 Privileged User Provisioning Use Case

This use case shows the transition of an unprivileged user to a privileged user with access to agency resources, per the user's entitlement and roles. This use case highlights the CDM functionality associated with Identity Management. CDM ILM, a sub-capability under PRIV, enables automation throughout the IDAM lifecycle by adjusting information in connected repositories to address changing user positions and responsibilities for privileged users. A user identity may exist prior to PIV issuance; however, CDM's primary focus is on employees and contractors who have obtained a PIV.

FICAM Reference: Motivated by FICAM Playbook Use Case 4, "Create and Issue a Credential."
Description: An unprivileged user makes a request to have privileged access to an agency's application.
Actors: User (employee or contractor), agency administrator, Identity Management system

Pre-condition: All users (with or without privilege) at the agency have a PIV card that must be used to authenticate the user's identity. A privileged user is required to use their PIV card to authenticate to the PAM solution to access the agency service.
Initial condition: The unprivileged user has a valid identity record and a valid PIV created via the PIV process.
Steps:

1. [FICAM] An unprivileged user requests privileged access to agency services. [1.1]
4. [FICAM] The user presents their PIV to the agency administrator. [1.1]
5. [FICAM] The user's PIV is verified, confirming the user's identity. [1.1]
6. [CDM] The agency administrator is notified because changes to necessary user privileges require approval. [ILM-2]
7. [FICAM and CDM] The agency administrator assesses the user's privileged access request based on the authoritative source information. [1.3, ILM-1]
8. [FICAM] If approved, the agency administrator adds the new privileged role to the user's identity record and updates the user's information in the agency's Identity Management system. [1.3, ILM-3]
9. [FICAM and CDM] The ILM provisioning process updates the user's identity record with the new entitlement and roles in the target applications and cloud directory service for cloud applications. [1.3, ILM-3]

Post-condition: Employee is successfully provisioned in the requested agency services.

6.1.3.2 Privilege Elevation Through Federation Use Case

The use case in this subsection describes the elevation of privileges by role selection through federation and use of CSPs.

FICAM Reference: Motivated by FICAM architecture Use Case 8, "Accept Federation Assertions."[43]
Description: In a hybrid cloud environment, an agency administrator employee has three administrative roles (Database Admin, Storage Admin, Web Application Admin) in an IaaS cloud service application. The agency administrator needs to perform database routine maintenance tasks in the cloud after regular business hours.
Actors: Agency administrator, existing PIV credential, agency Identity Provider (IdP) [e.g., AD with Federated SSO Service (ADFS)], Target Cloud Service, Target System,)
Pre-condition: The agency hosts an IdP on-premises that supports federated SSO for user authentication. The agency IdP has established the identity trust relationship with the CSP as the relying party. The administrator has a PIV card as their credential for user authentication. The agency administrator has the following attributes in their identity records in the agency IdP for privileged access in the cloud application:

- DB Admin
- Storage Admin
- Web App Admin

The Cloud Service Access Control System has the following roles configured:

- Database Administrators
- Storage Administrators
- Web Application Administrators

Steps:

[43] General Services Administration. "The Federal Identity, Credential, and Access Management Architecture," Version 3.1, FINAL. January 6, 2021, accessed May 20, 2022. https://playbooks.idmanagement.gov/docs/ficam-arch.pdf.

1. [FICAM] The administrator initiates an access request through the browser to access the cloud application.
2. [FICAM and CDM] The cloud application evaluates the incoming privileged access request and forwards the browser with a Security Assertion Markup Language (SAML) request to the agency's trusted IdP.
3. [FICAM] The browser is redirected to the agency SSO interface for user authentication.
4. [FICAM] The agency administrator's PIV is verified and confirmed as the identity.
5. [FICAM and CDM] The agency IdP evaluates the agency administrator's identity records and adds the privileged attributes as the SAML assertion.
6. [FICAM] The agency IdP forwards the browser with a signed assertion as the SAML response token to the cloud service.
7. [FICAM] The cloud application evaluates the SAML token and confirms that the token is issued by the trusted IdP.
8. [FICAM] The cloud application verifies the SAML assertions included in the SAML token.
9. [FICAM and CDM] The cloud application extracts and evaluates the available attributes included in the SAML token and maps the attributes to the privileged roles (i.e., database administrators, storage administrators, web application administrators).
10. [FICAM and CDM] The administrator's browser is directed to an access portal page with options to select a role.
11. [FICAM and CDM] The administrator selects the database administrator's role and submits.
12. [FICAM and CDM] The cloud application authorizes the agency administrator to perform the task as the database administrator.

Post-condition: The Administrator has completed the administrative task. CDM monitors steps above as indicated, and reports deviations from the expected states.

6.2 CREDENTIAL MANAGEMENT

A credential authoritatively binds a digital identity to an entity (PE or NPE). It is then used by that entity to authenticate its identity claim to a third-party application (e.g., AD) by demonstrating possession and control of the credential. Credential Management is how an agency issues, manages, and revokes credentials bound to enterprise identities.[44] Credential Management creates, issues, and maintains objects (e.g., credentials and tokens) that authoritatively bind an identity and attributes to a token processed and controlled by an entity. FICAM and NIST SP 800-63B have general guidance for secure Credential Management, for PE including how to support post-enrollment binding of an authenticator described in NIST SP 800-63B. NIST SP 800-63C describes the use of federation protocols and the associated assertions and session management.

FIPS-201-3 states the policies and minimum requirements of a PIV card and PIV-D credentials issued to a PE that allow interoperability of credentials for physical and logical access. It specifies the use of federation protocols as a means of accepting PIV cards and PIV-D credentials issued by other agencies.

A PIV card is the result of Identity Proofing and identity vetting. After Identity Proofing and initial identity vetting is complete (not a complete background investigation), a digital certificate with the person's identity information is issued on the PIV card. The digital certificate on the PIV card is bound to an identity record in the agency's Enterprise Identity Management system.

A key theme in OMB Memo 19-17 is for federal agencies to shift the focus from managing the lifecycle of credentials to managing the lifecycle of identities. In line with the terms of Executive Order 14028 requiring that agencies "adopt multi-factor authentication … to the maximum extent" and Executive Order 13681 requiring "that all agencies making personal data accessible to citizens through digital applications require the

[44] General Services Administration. "The Federal Identity, Credential, and Access Management Architecture," Version 3.1, FINAL. January 6, 2021, accessed May 20, 2022. https://playbooks.idmanagement.gov/docs/ficam-arch.pdf.

use of multiple factors of authentication," the agency must implement MFA at AAL2 or AAL3. (NIST SP 800-63-3) Where PIV is not required or not practical, agencies issuing MFA will apply the IAL appropriate for the AAL of the MFA.

CDM Relationship to Credential Management: CDM receives input from the TRUST capability as a result of the FIPS 201-3-defined adjudication process.

The Credential Management functions shown in Figure 6-3 are described in the following subsections. The primary functions that support issuing a new credential include Credential Sponsorship, Credential Registration, Provisioning, and Credential Generation and Issuance. The functions supporting the reissuance of a credential include the Credential Maintenance, Credential Generation, and Issuance functions, and the Credential Revocation function supports revoking the use of a credential. Each of these cases would require an update to the credential repository.

CDM supports Credential Management through the establishment of credential desired-state information in the form of machine-readable policies, through the collection of actual credential data from authoritative sources, and through comparing these two sources of information to identify discrepancies. These credential discrepancies are displayed succinctly at the agency level and with more details at the local level.

CDM collects agency CRED desired-state information and actual-state information, compares the two, and reports the information to the dashboard. For NPE credentials, CDM observes that they are created and managed by an authorized user or group of authorized users through the PRIV and PAM capability area.

It is anticipated that TRUST may be updated to provide Continuous Vetting capabilities as specified in EO 13764, which occurs when the Identity Proofing and/or vetting is complete when those services are available. This may result in action required on the CRED object.

6.2.1 Assumptions and Constraints

The following assumptions apply to Credential Management. Credential Management assumes PIV and PIV-D credentials are issued in accordance with FIPS 201-3, NIST SP 800-157, and NIST SP 800-63-3, or other guidance.

Based on HSPD-12, all PIV cards, PIV-D credentials, and other MFA, regardless of their composition, must meet the following criteria:

- They are issued based on sound criteria for verifying an individual employee's identity.
- They are strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation.
- They can be rapidly authenticated electronically.
- They are issued only by providers whose reliability has been established by an official accreditation process.
- Tier 1 investigation is complete and adjudication is continuously validated.

CDM-Related Functionality: For NPE, CDM evaluates the creation within the PRIV and PAM capabilities.

6.2.2 Functions

The Credential Management functions shown in Figure 6-3 are described in the following subsections. For each function, a general description is provided, as well as CDM's support of that function, as applicable.

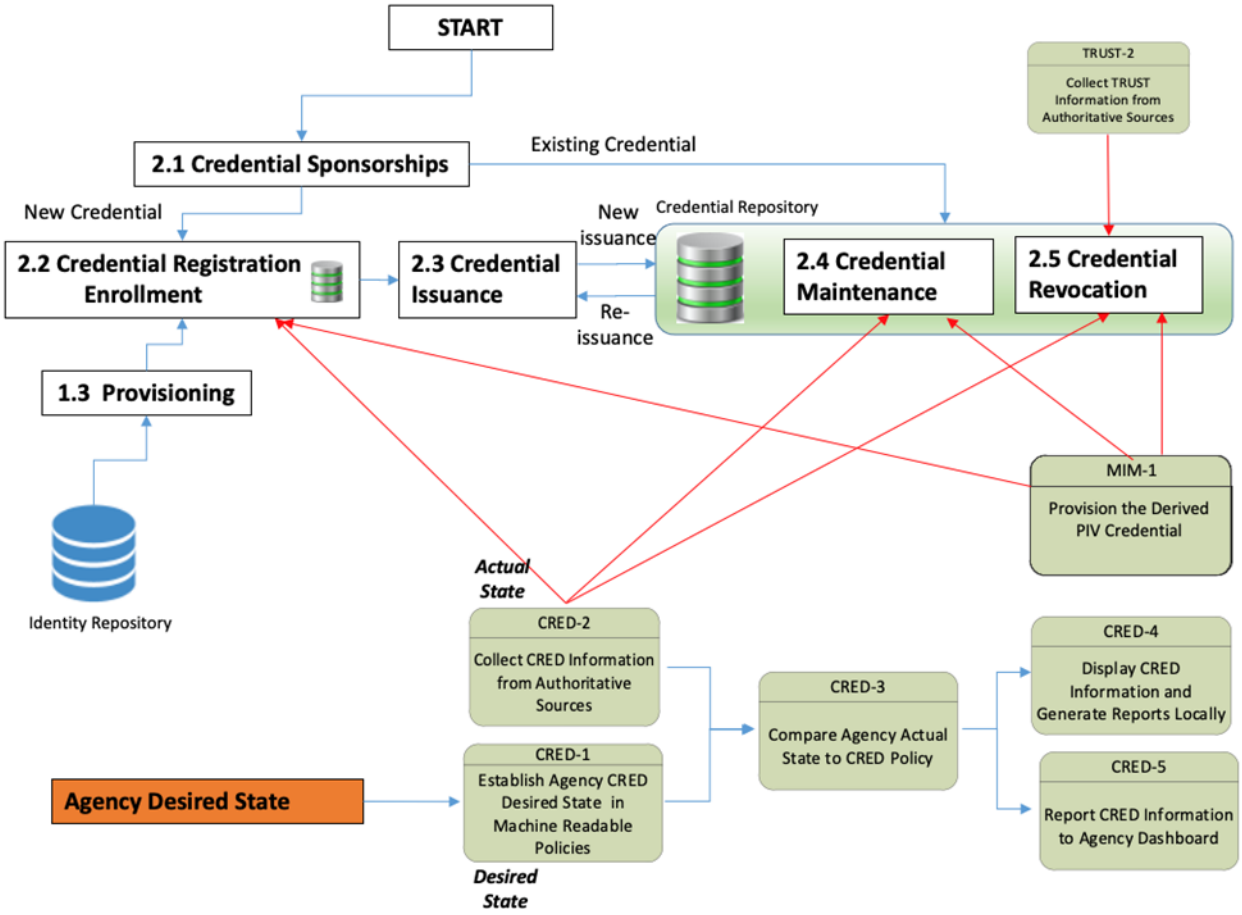


Figure 6-3: Credential Management Functional Block Diagram

6.2.2.1 Credential Sponsorship

The Credential Sponsorship function formally establishes the authorized need for credentialing an entity.[45] Sponsorship may occur as part of Identity Management or may be performed independently as part of Credential Management.[46]

CDM-Related Functionality: None.

6.2.2.2 Credential Registration and Evaluation

Individuals being processed for a PIV credential shall receive the required investigation (described in FIPS 201-3) and are subject to any applicable reinvestigation or continuous vetting requirements to maintain their PIV eligibility. The Credential Registration function collects the information needed from a person or entity to issue them a credential.[47] Entities may have identities managed outside agencies, but are issued credentials by

[45] General Services Administration. "The Federal Identity, Credential, and Access Management Architecture," Version 3.1, FINAL. January 6, 2021, accessed May 20, 2022. https://playbooks.idmanagement.gov/docs/ficam-arch.pdf.
[46] Department of Defense. "DoD Enterprise Identity, Credential, and Access Management (ICAM) Reference Design," Version 1.0, June 2020, accessed July 25, 2023, https://dodcio.defense.gov/Portals/0/Documents/Cyber/DoD_Enterprise_ICAM_Reference_Design.pdf.
[47] General Services Administration. "The Federal Identity, Credential, and Access Management Architecture," Version 3.1, FINAL. January 6, 2021, accessed May 20, 2022. https://playbooks.idmanagement.gov/docs/ficam-arch.pdf.

external, approved credential providers. These need to be registered in an entity data repository to use their external credentials.[48]

Derived PIV credentials are additional PIV credentials that are issued based on proof of possession and control of a PIV card. Derived PIV credentials should be bound to the cardholder's PIV identity account only by the agency responsible for managing that PIV identity account. Both PIV and PIV-D credentials need to be registered in an entity data repository. For further discussion on credentialing requirements for federal departments and agencies, see FIPS 201-3 Section 2.2.

CDM-Related Functionality: None.

6.2.2.3 Credential Generation and Issuance

The Credential Generation and Issuance function assigns a credential to a person or entity.[49] The function correctly and securely creates, issues, verifies, and maps identities to attributes (see NIST SP 800-63A and FIPS 201-3). For security and mission-critical systems, a second factor or device should be used. Authenticator and token characteristics [e.g., minimum password or personal identification number (PIN) length, validation time window for time-synchronous one-time tokens, and number of allowed rejections during the verification stage of biometric authentication] should be specified at the agency level. Actions should be taken to safeguard individual authenticators, including maintaining possession of authenticators, not sharing authenticators with others, and immediately reporting lost, stolen, or compromised authenticators.
NPE credentials provide privileged functions and proof that the identity is tightly coupled to accounts generated within the PRIV and PAM functions and should be stored securely. Secrets associated with the NPE credentials should be stored encrypted or in an external service or hardware security module where they are retrieved upon use.

CDM-Related Functionality: CDM assumes that agencies have accepted an employee or contractor to operate within their environment (usually through FIPS 201-3-related processes) and have registered them with acceptable PIV or PIV-D credentials.

6.2.2.4 Credential Maintenance

The Credential Maintenance function maintains a credential throughout its lifecycle.[50] Some maintenance examples include renewal, re-keying, or modification of the credentials.[51]

CDM-Related Functionality: CDM monitors status of the PIV card and PIV-D credentials, as reported by the authoritative sources, and can trigger on failure of the desired-state comparison.

6.2.2.5 Credential Revocation

The Credential Revocation function will revoke a credential from a person or entity or deactivate an authenticator.[52] Credentials should be revoked based on expiration date, being lost, or being invalidated, per agency policy.

CDM-Related Functionality: CDM monitors status of the PIV card and PIV-D credentials as reported by the authoritative sources and can trigger on failure of the desired-state comparison.

---

[48] Department of Defense. "DoD Enterprise Identity, Credential, and Access Management (ICAM) Reference Design," Version 1.0, June 2020, accessed July 25, 2023, https://dodcio.defense.gov/Portals/0/Documents/Cyber/DoD_Enterprise_ICAM_Reference_Design.pdf.
[49] General Services Administration. "The Federal Identity, Credential, and Access Management Architecture," Version 3.1, FINAL. January 6, 2021, accessed May 20, 2022. https://playbooks.idmanagement.gov/docs/ficam-arch.pdf.
[50] Ibid.
[51] Executive Office of the President, Federal Chief Information Officers Council. "Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, Version 2.0," December 2, 2011, accessed July 25, 2023, https://playbooks.idmanagement.gov/docs/roadmap-ficam.pdf.
[52] General Services Administration. "The Federal Identity, Credential, and Access Management Architecture," Version 3.1, FINAL. January 6, 2021, accessed May 20, 2022. https://playbooks.idmanagement.gov/docs/ficam-arch.pdf.

It is anticipated that TRUST may be updated to provide Continuous Vetting capabilities as specified in EO 13764, which occurs when the Identity Proofing and/or vetting is complete when those services are available. This may result in action required on the CRED object.

6.2.3 Use Cases

6.2.3.1 Re-Issue a Credential (Replace a lost Credential) Use Case

FICAM Reference: Motivated by FICAM Playbook Use Case 4, "Create and Issue a Credential."
Description: An individual (employee or contractor) who lost their credential requests a new credential from an agency.
Actors: Employee, administrator or supervisor, identity repository, and credential repository
Pre-condition: Employee is new to the agency and requests credentials to access agency services.
Steps:

1. [FICAM] An individual requests a new credential from the agency to access specific agency services. [2.1]
2. [FICAM] The agency administrator confirms the individual's identity and assesses the user's suitability. [1.1]
3. [FICAM] The individual is approved by the agency supervisor to receive a credential. [2.1]
4. [FICAM] The individual is enrolled in the agency's credential enrollment system. [2.2]
5. [FICAM] The agency collects the applicant's information required for enrollment from the identity repository. [2.2]
6. [CDM] The CRED desired-state data are collected from the authoritative sources. [CRED-1]
7. [CDM] CDM collects the individual's actual-state CRED information, which may include attributes used to access agency systems and networks. [CRED-2]
8. [FICAM and CDM] The Identity Management system reports the request and approval information to the CDM CRED and PRIV functions. [2.1] [CRED-2]
9. [FICAM and CDM] Credentials are issued to the applicant and stored in the credential repository and reported to CRED and PRIV. [2.3] [CRED-2]

Post-condition: Employee successfully receives a new credential. CRED and PRIV collect applicable reissuance data.

6.2.3.2 Revoke a Credential Use Case

FICAM Reference: Motivated by FICAM Playbook Use Case 4, "Create and Issue a Credential."
Description: An individual (employee or contractor) requests the agency to revoke a lost credential.
Actors: Employee, administrator or supervisor, identity repository, and credential repository
Pre-condition: Employee has lost a valid credential and needs to revoke it.
Steps:

1. [FICAM] An individual requests the agency to revoke the lost credential. [2.1]
2. [FICAM] The agency administrator confirms the individual's identity and assesses the user's suitability. [1.1]
3. [FICAM] The individual is approved by the agency supervisor to revoke the lost credential. [2.1]
4. [FICAM] The agency administrator revokes the lost credential and updates the information in the credential repository. [2.4]
5. [FICAM and CDM] The CDM CRED and PRIV functions collect the updated information on the next scan. [2.1] [CRED-2]
6. [FICAM] The individual is issued a new credential.
7. [CDM] The CDM CRED function compares the actual state and the desired state of the individual's credential, and provides information, including defects, to the CDM Agency Dashboard. [CRED-3, CRED-4, CRED-5]

Post-condition: Employee successfully revokes a lost credential; the employee receives new credentials, if necessary. This will be captured by CDM in the required CRED-ACCOUNT metric, see Section 6.4. CRED and PRIV collect applicable revocation data.

6.2.3.3 Issue NPE Credentials Use Case

FICAM Reference: Motivated by FICAM Playbook Use Case 4, "Create and Issue a Credential."
Description: This use case flow provides the high-level process steps for an agency to establish a credential for an NPE that will be used to access the agency's protected resources. Credential types that support the NPEs in common practice and are discussed in this use case are PKI-based software tokens, username and password, or authentication secret (as defined in NIST SP 800-63-3). A certificate issued to an agency user's workstation, or a network-connected device (such as a printer) is a typical example of using a PKI-based credential for NPE.
Use Case: A new NPE is requested by an application administrator to support the system or application.
Actors: Agency administrator, supervisor, application owner, NPE owner, Credential Management system, key management system
Pre-condition: The NPE has an established Identity Record with Access Control Profile. An authorized credential request has been generated.
Steps:

1. [FICAM] The agency administrator authenticates and verifies the authorized credential request. [2.1]
2. [FICAM] The agency administrator uses the Credential Management system to create a credential for the NPE with the necessary information of the NPE based on the credential type. [2.2][2.3]
   a) *For username- and password-based NPE:* A username that is unique and identifiable in the NPE Identity Record. The username and password can be local to the hosting system or global to the network infrastructure. The agency PAM capability should manage the password and the password lifecycle per agency policy.
3. [CDM] Establish CRED information with the following NPE credential information from the authoritative sources. CDM will collect and update this CRED information. [CRED-1],[CRED-2]
   a) *For username- and password-based NPE credential:* Username; timestamp of the latest password renewal, and next password renewal schedule enforced by agency policy; application information, including the endpoints or interfaces where the credential is applied
4. [CDM] Establish or update agency CRED desired state in machine-readable policies to include the NPE credential information.
5. [FICAM] The agency administrator officer will evaluate the Access Control Profile of the NPE and determine whether the credential should be enrolled to the agency's PAM system (like CyberArk) for credential maintenance per agency policy.
6. [FICAM] The application owner installs and activates the credential in the application.
7. [FICAM] The agency administrator notifies the NPE owner that this change has occurred.

Post-condition: The NPE is enrolled, and a credential is established. This will be captured by CDM in the proposed PRIV-REV metric; see Section 6.4. CRED updates the NPE desired state of the credential information.

6.2.3.4 Issue a Derived Credential Use Case[53]

FICAM Reference: Leveraged from DHS Derived PIV Working Group. Implementations may vary.
Description: An individual (employee or contractor) requests a derived credential from an agency.
Actors: Employee, Identity Management System (IDMS)/Credential Management System (CMS), Master Data Management (MDM), Certification Authority (CA)
Request Phase Pre-condition: Agency pre-provisions mobile devices prior to issuing the device to the user, or holder. The devices have MDM clients installed. The device has an identity, and the holder's identity is bound to the device. Connections between the device and the Enterprise MDM are secured and mutually authenticated. The MDM knows the device to which it is connected and, consequently, the identity of the holder. The device is also provisioned with the PIV-D mobile application the first time the user goes through the

[53] Content for this subsection is from https://community.max.gov/display/Egov/Derived-PIV+Use+Cases+Repository.

PIV-D request process. The application's provisioning allows it to securely communicate with the Enterprise MDM. The application and MDM mutually authenticate. The MDM knows the identity of the application and, consequently, the user's identity. However, the application is not provisioned with the DPC. When requesting a PIV-D, the user must employ a DHS workstation securely connected to the agency network (e.g., physical connection in DHS facility or remotely through a DHS VPN). The device must have a PIV card reader. The user must have a currently active, valid PIV card.

The use case has two phases: a request phase and an issue phase, both outlined next.

Request Phase Steps:

1. [FICAM] The user signs into the DHS network.
2. [FICAM] The user authenticates to the network with their PIV card.
3. [FICAM] The user opens a browser to the IDMS Portal PIV-D request page and requests a DPC. The CMS authenticates the user's PIV card.
4. [FICAM] The IDMS/CMS confirms that the PIV is valid (e.g., certificate has valid signature, asserts PIV-authorization policy, is within its validity period, and has not been revoked).
5. [FICAM] The IDMS/CMS requests from the MDM a list of devices that have been issued to the user.
6. [FICAM] The MDM responds with the device list.
7. [FICAM] The IDMS Portal presents the user with a list of devices and asks the user to identify the target device.
8. [FICAM] The user selects the target device and accepts the agreement regarding use of the DPC.
9. [FICAM] The CMS acknowledges completion of the DPC request. At this point the user's involvement in the request is complete.
10. [FICAM] The CMS prepares the DPC in advance of the user's request to install it on the device. The CMS generates the DPC's public key (PK) pair and prepares a certificate signing request (CSR).
11. [FICAM] The CMS sends the CSR to the CA to request a PIV-D certificate.
12. [FICAM] The CA creates and returns the certificate.
13. [FICAM] The CMS creates a "payload" that wraps the DPC (i.e., PK pair and certificate).
14. [FICAM] The CMS sends the payload to the MDM.

Issue Phase Pre-condition: The mobile device is necessary for the issue phase and must have internet connectivity (e.g., either cell phone or Wi-Fi connectivity). The workstation is not necessary. The user must have previously requested the DPC. The "same" DPC will be installed in two places on the device. One instance will be available to applications belonging to the MDM (but not Apple iOS applications such as Safari and mail). The Apple applications can access the other instance.

Issue Phase Steps:

1. [FICAM] The user unlocks the device (using PIN or biometric).
2. [FICAM] The user launches the PIV-D application and requests the DPC. The PIV-D application establishes a mutually authenticated, secure channel with the MDM and requests the DPC. The application is able to establish this secured connection because DHS provisioned the device for the specific user when it issued the device to the user.
3. [FICAM] The MDM identifies the device and retrieves the appropriate payload created at the end of the request phase.
4. [FICAM] The MDM returns the payload.
5. [FICAM] The PIV-D application installs the DPC in the iOS keychain. This DPC instance can only be used by applications developed by VMWare as the PIV-D application.
6. [FICAM] The PIV-D creates an encrypted configuration profile containing the DPC.
7. [FICAM] The PIV-D transmits the profile to the MDM.
8. [FICAM] The MDM digitally signs the profile and sends it to the MDM client.
9. [FICAM] The device authenticates the MDM as the source and installs the DPC in the system iOS keychain. The Apple native applications (e.g., Safari, mail) have access to this DPC instance.

Post-condition: Employee successfully receives a derived credential. CDM will capture the required CRED-ACCOUNT metric as part of the post-condition; see Section 6.4.

6.3 ENTITY AND PRIVILEGED ACCESS MANAGEMENT

6.3.1 User (Entity) Access Management

Access Management is how an agency authenticates enterprise identities and authorizes appropriate access to protected services.[54] Access Management will grant or deny specific requests to obtain and use information from agency resources, as well as allow physical access to facilities. Access Management grants or denies specific requests to: (1) obtain and use information and related information processing services; and (2) enter specific physical facilities (e.g., Federal buildings, military establishments, border-crossing entrances). Although it is common for a credential to serve as an entrance token, the capability's main function is to authenticate and authorize entity permissions against a logical resource. (See FICAM, NIST SP 800-53 and NIST SP 800-162.) Access Management covers PE and NPE.

Access Management provides the management and control of the ways in which entities are granted or denied access to resources. The purpose of Access Management is to ensure that the proper identity verification is made when an individual attempts to access protected resources.

Access Management leverages identities, credentials, and privileges to determine access to protected resources by authenticating credentials. After authentication, a decision as to whether the individual is authorized to access the resource can be made.

A policy is a set of agency rules that defines who is authorized to have secure access to the protected resources. A policy can be created and managed through an enterprise Policy Administration Point. Once created, an enterprise PDP will evaluate the policy to make an access decision. The decision can be delivered to the PEP at the protected resources to enforce access control.

In Access Management, there are four basic access control models: Access Control List, Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), and Policy-Based Access Control. Each of these authorization models has benefits and limitations.

6.3.2 Privileged Access Management

PAM protects access to accounts that have access permissions that can effectively change IT system configurations and data security. After a user has been authenticated (i.e., who they claim to be has been confirmed), they must be authorized to access the resources they seek. In RBAC and ABAC, an authorization engine requires access to attributes that describe users' privileges. In RBAC, these privileges are conveyed in terms of user roles, with defined responsibilities. In ABAC, these privileges are defined in terms of specific access to resources that are necessary to get a particular job done. Such privileges have been provided only after a user completes data handling training by some agencies. ABAC attributes describe resources in terms that include data sensitivity or classification, which can be compared with user privilege attributes based on training, to establish access control. Both RBAC and ABAC require the use of a PDP which reflects up-to-date policies and applies that information, along with the user and resource attributes, in making an access control decision to allow or deny access.[55]

Access control functions, shown on the right side in Figure 5-8, will be initiated from Identity Management and Credential Management. Access Management is enabling these controls to be localized for the decision or to allow querying the sources at runtime. CDM is involved in the authentication of a privileged user's access through the PAM tool functionality, validating accounts and authorizing revised access privileges. CDM compares an agency's TRUST, BEHAVE, and PRIV desired states (which are retrieved from the agency policies)

[54] General Services Administration. "The Federal Identity, Credential, and Access Management Architecture," Version 3.1, FINAL. January 6, 2021, accessed May 20, 2022. https://playbooks.idmanagement.gov/docs/ficam-arch.pdf.
[55] DHS Science and Technology, "Identity, Credential, and Access Management (ICAM) Acquisition Guidance," Version 2, February 2019, https://www.dhs.gov/sites/default/files/publications/icam_acquisition_guidance_final_version_-_092019.pdf.

to actual states, and will report defects to the dashboard as well as provide local reports. CDM ILM can maintain "entitlements," which can be used to make access control decisions when made available to the Access Controller. CDM ILM can prevent provisioning accounts to the Access Management system when agency policies are not met by comparing TRUST, BEHAVE, and PRIV information with agency policies. The numbered functions with a white background are traditional ICAM functions, whereas the functions in gray shading are federated functions.

CDM Relationship to Access Management: The lower part of Figure 6-4 (which is a companion to Figure 5-8) outlines the relationships and outcomes from the comparative processing of the agency desired state to the agency actual state for PRIV, BEHAVE, and TRUST. Note the various functions supporting the policies, which are shown at the bottom. All but the Federated Access Manager, shown with gray shading, are in scope for ICAM.

The data dictionary in the current CDM DMD defines the specific attributes for IDAM to support a Policy Administrative Point to define and manage the machine-readable policies (desired state). By comparing the agency policy-based desired state with the collected actual-state attribute values from authoritative sources, the CDM PRIV capability detects anomalous activities or policy violations in a PDP that enforces the access control decision on the PEP. However, this access management functionality is only limited to managing privileged user access. The current CDM ICAM capabilities do not have functions or tools that support access control decisions for regular users. The current CDM IDAM capabilities only monitor the regular user activities and report anomalous activities to the agency and federal dashboards.

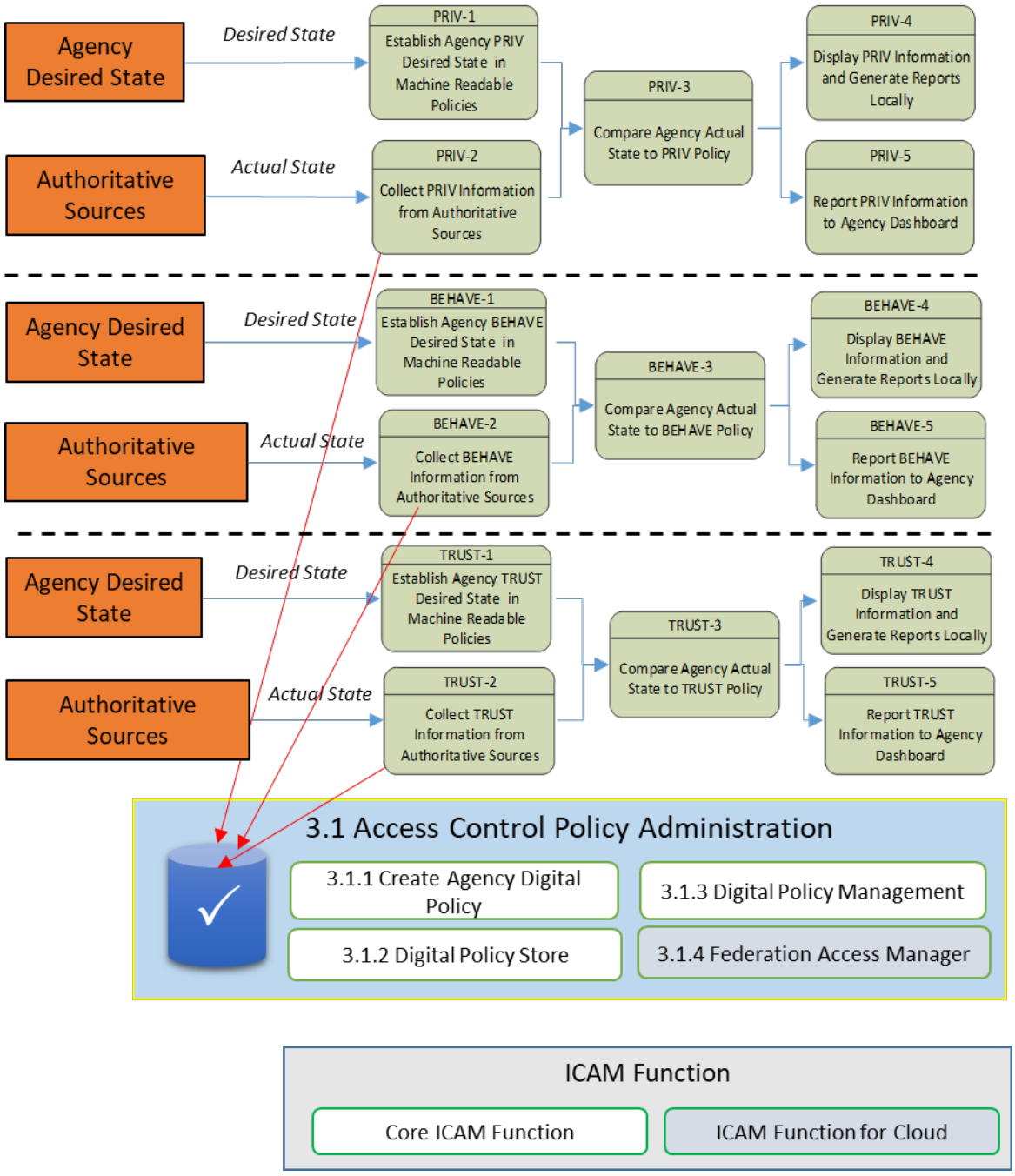


Figure 6-4: Access Management Functional Block Diagram

6.3.3. Zero Trust Architecture – Dynamic Access Control and Other Signals

In a ZTA, multiple pillars combine to provide richer context in which to make an access control decision. For instance, a user must be authenticated to the device and the device should have its security posture evaluated and reported to the PDP before an access request to an enterprise-owned resource is granted by the PEP. The CDM Asset Management Capability Area focuses on identifying and monitoring agency devices, ensuring they are known devices with appropriate software configured such that vulnerabilities have been identified and remediated; capability area, shown in Figure 6-5, includes the HWAM, SWAM, and VUL capabilities. The HWAM and SWAM functions help agencies identify known devices on their network infrastructure and SWAM functions

provide the agencies with software inventory to determine the current and desired state of software on the device. The VUL function provides information about the existence of known vulnerabilities on the device. In a Zero Trust environment, this information could be conveyed to the PDP from an EMM, from an EDR solution, or from other sensors deployed in the environment.

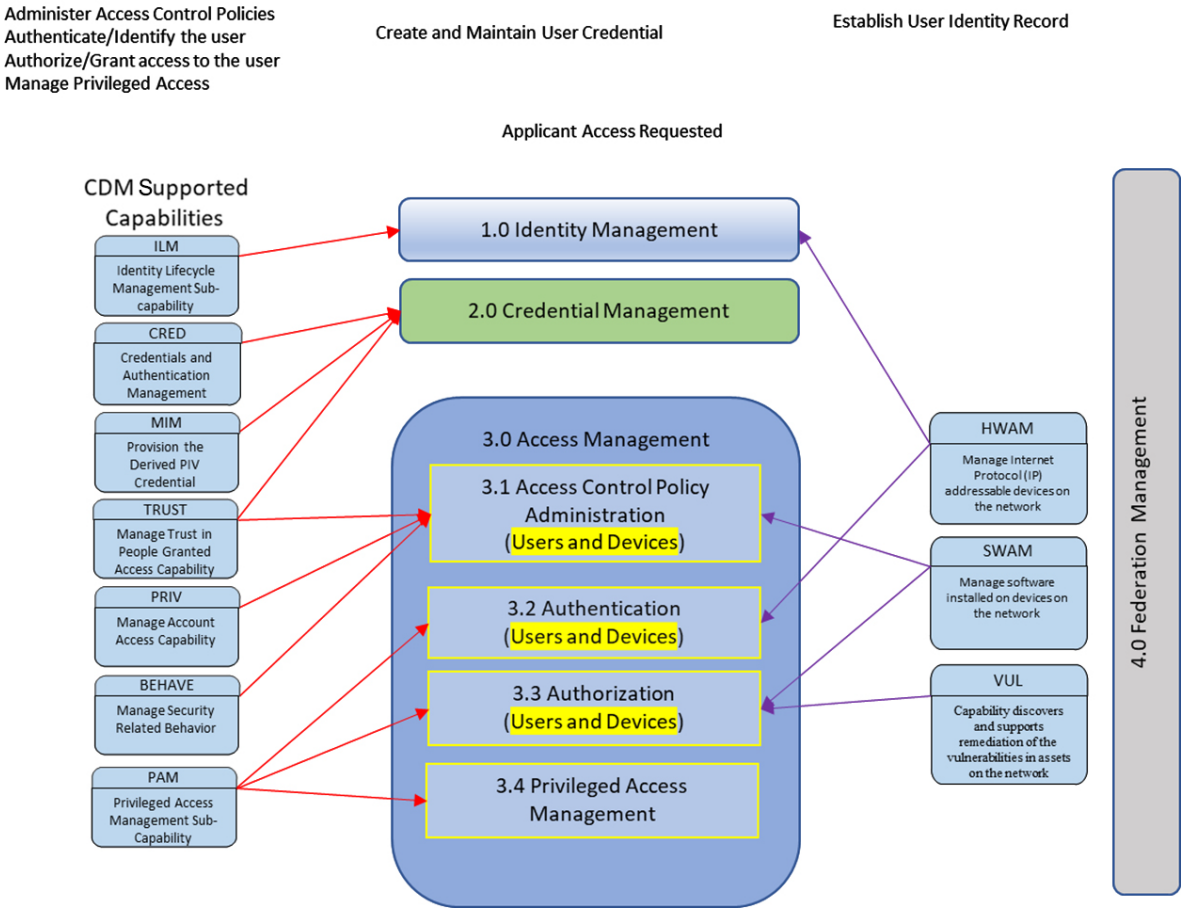


Figure 6-5: Asset Management and NAC Functional Block Diagram

6.3.4 Assumptions and Constraints

The assumptions of the use of technology and constraints that apply to agency internal Access Management and Access Management between agencies cover many facets of the process, including an authentication event and an authorization event. Several categories of related assumptions are as follows:

- **Authentication** Assumptions for Non-Admin and Admin Users
  - Although authentication is considered distinct from authorization, it is important to note that an authorization event is always preceded by an authentication event. The presentation of a valid authenticator to provide authentication, followed by authorization, is typically considered the first step of the authorization management process.
  - Multi-factor cryptographic device authenticators are supported by tamper-resistant hardware.
  - A PKI certificate with a secret PIN is used, which unlocks a private key embedded in a PIV card.
  - Non-PKI MFA and PK authentication with external infrastructure are used.
  - NIST SP 800-63B provides AAL evaluation guidance, which applies to the MFA.
  - Agencies ensure MFAs that have been evaluated and meet the AAL2 or AAL3 requirements of NIST SP 800-63B are procured.

  - Agencies also ensure that the other members of the Access Management Federation are able to authenticate their entities using MFA, which may include a redirect to the issuing agency's IdP to support out-of-band factors.
  - NPE credentials are either based on PK cryptography or securely stored in, and programmatically retrieved from, the PAM secrets vault.
  - See CDM Technical Capabilities, Volume 2 Requirements on CRED for further details on authentication.
- **Attribute** Assumptions for Admin Users
  - Attribute management
    - Entity attributes are accurate and accessible when needed by the access control system (ACS), including federated access management support, which should give near-real-time access.
    - User profile attributes may include permission, roles, groups, or custom attributes. Password hashes associated with user profiles typically remain on-premises instead of being propagated to an IdP or federation gateway.[56]
    - Privileged users have organizational "role" designations that express the privilege scope.
  - Session-based attributes
    - Session-based attributes should align with NIST SP 800-63C and related updates.
    - CDM will primarily be focused on providing attributes and not on the use of the attributes.

6.3.5 Access Management Functions

The Access Management functions shown in Figure 6-4 and Figure 6-5 are described in the following subsections. For each function, a general description is provided, as well as CDM's support of that function, as applicable.

The Access Management functions shown in Figure 6-6 describe a modern SP-initiated authentication flow that is common in a modern SSO environment.

1. User attempts to log into a cloud application.
2. The Service Provider (SP) federation services checks to see if there is a valid, active session.
3. If no session exists, the federation service redirects back to the browser, which then makes a request for the user to authenticate at the Identity Provider (IDP).
4. The IDP performs the authentication by interacting with the user and the presentation of credentials and verifies the information in the Identity records that the IDP holds.
5. The IDP returns to the user client an identity assertion, which is then forwarded to the SP in the form of an Identity Assertion.
6. If the SP is satisfied that the user meets requirements, it can authorize the use of that assertion at the cloud application.

Access control patterns similar to this will be part of a Zero Trust authentication flow and may be enhanced by signals from other systems, such as device health signals, as a dynamic access control decision as described in Section 6.3.3.

[56] Department of Homeland Security. "Continuous Diagnostics and Mitigation (CDM) Program Cloud Guidance Document, Volume 1, Architecture, Data Flows, and Data Sources," Version 2.0, May 2020.

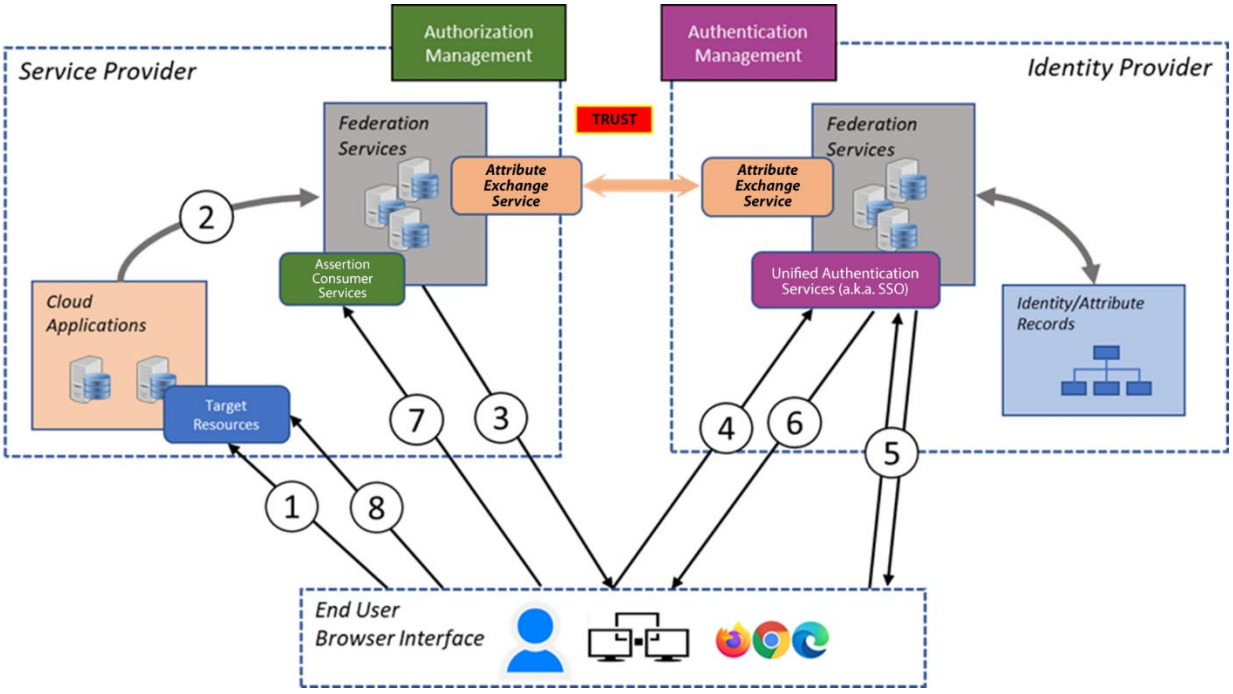


Figure 6-6: SP-Initiated User Access to Cloud Application

6.3.5.1 Policy Administration

The Policy Administration function creates and maintains the technical access requirements that govern access to protected agency services.[57] Policy Administration only accepts policy from trusted sources, validates the policy, and stores the policy in a protected repository. The function must keep access control policy current.

Policy Administration consists of the following:

- Create Agency Digital Policy: Creates the rule sets that meet the access requirements to control the access decision to the protected resources.
- Digital Policy Management: Maintains the digital policies, including policy lifecycle, modifying, updating, and deleting.
- Digital Policy Store: Provides data storage or a repository with restricted access control to store digital policies. (CDM will query the policy repository for its actual state.)
- Federated Access Manager: Provides sharing and trust services that enable brokered and peer-to-peer transactions.

CDM-Related Functionality: CDM maintains policy for privileged users in addition to querying the policy repository for the actual state.

6.3.5.2 Privileged Access Management

The PAM function ensures only authorized entities can perform actions against controlled resources. Privilege is a right granted to an individual, program, or process (entity). An entity granted no rights is considered to have no privileges.

In the case of an NPE that has access permissions that can affect system-level or application-level configurations and data security (such as acting as a service account to run applications or service requests, or

[57] General Services Administration. "The Federal Identity, Credential, and Access Management Architecture," Version 3.1, FINAL. January 6, 2021, accessed May 20, 2022. https://playbooks.idmanagement.gov/docs/ficam-arch.pdf.

affecting systems accounts at a system level, such as local printers or global infrastructure), access to the NPE account should be protected and managed properly, such as through the secrets vault of the agency PAM solution (such as CyberArk). Activity sessions of an NPE account with privileged access should be monitored, and the NPE's password or secrets lifecycle should be managed and automated through the agency's PAM solution to minimize risks. When collecting the NPE event activity information from the PAM solution, CDM compares the actual access state of the NPE account with the agency's desired states and will report the information to the Agency Dashboard.

Identifiers are mapped to PEs and NPEs and are stored in a source system of record. The record should be centrally managed and protected to the same assurance level of the access provided by the identifier.
In the case of NPEs, information provided on behalf of the NPE shall include the PE to which the NPE device or account is assigned. NPE can perform privileged functions, and their identity is tightly coupled to accounts generated within the PRIV and PAM functions. NPE accounts are only valid for the period that the PE identity remains valid in the system.

CDM-Related Functionality: Identity Proofing varies based on the type of NPE. CDM assumes an NPE sponsor has verified the NPE identity prior to issuing an account to the NPE. Identity Proofing is a prerequisite for the CDM CRED and ILM functions.

6.3.6 Use Cases

There are two use cases for granting access: one for a PE, and one for an NPE.

6.3.6.1 Grant Access for PE Use Case

FICAM Reference: Motivated by FICAM Architecture Use Case 7, "Grant Access."
Description: A systems administrator employee needs privileged access to perform routine administrative tasks.
Actors: Administrator, existing PIV credential, agency Identity Store (e.g., AD), target system, agency security key vault system, agency ACS
Pre-condition: The administrator has a PIV card as their credential. The administrator has access to the security key vault system. The administrator is authorized to use a privileged credential stored in the security key vault to perform an administrative task for a target system. The agency security key vault system is integrated with the agency enterprise identity store. The privileged credential for the target system is stored and managed by the agency's security key vault system.
Steps:

1. [FICAM] The administrator uses their PIV card to log onto the security key vault system.
2. [FICAM and CDM] The ACS verifies the PIV card and authenticates the administrator. [3.2.1, PAM-1]
3. [FICAM and CDM] The ACS verifies the access control policies of the administrator, and access is granted. [3.2.2, PAM-3]
4. [FICAM] The administrator checks out the privileged account credential authorized by the access control policies.
5. [FICAM] The administrator uses the privileged account credential to access the target system to perform the administrative task.
6. [FICAM] The administrator completes the administrative task and checks in the privileged account credential.
7. [FICAM] The security key vault system updates the privileged account credential with a new "secret" and updates its status (e.g., renewal information).
8. [FICAM] The security key vault system updates the privileged account credential in the agency Identity Store (e.g., AD) that is cryptographically based on the new secret.
9. [CDM] The CDM system updates the desired state of the privileged account stored in the agency Identity Store with the updated information (e.g., account renewal information).
10. [CDM] The CDM system updates the desired state of the privileged account stored in the security key vault system with the secrets renewal information.

Post-condition: The administrator has completed their administrative task. The privileged account credential is updated with a new secret. This will be captured by CDM in the proposed PRIV-REV metric, see . CDM monitors steps above as indicated, and reports deviations from the expected states.

6.3.6.2 Grant Access for NPE Use Case

FICAM Reference: Motivated by FICAM Architecture Use Case 7, "Grant Access."
Description: An administrator needs to change the password or secret of a service account (NPE credential) that supports an application hosted on a target system. The password or secret is managed by the agency security key vault system.
Actors: Administrator, service account (target NPE), agency Identity Store (e.g., agency AD), target system, target application, agency security key vault system, agency ACS
Pre-condition: The agency security key vault system has kept the current secret of the NPE's credential. The agency security key vault system has the capability to generate a randomized secret or password based on agency policy. The agency security key vault system is integrated with the agency Identity Store (e.g., agency AD). The agency security key vault system is also integrated with the target system. The key vault administrator can access the agency Identity Store as the administrator. The key vault administrator can access the target system as the administrator.
Steps:

1. [FICAM] The agency administrator logs into the agency security key vault system with a PE privileged credential (e.g., PIV card).
2. [FICAM and CDM] The ACS verifies the credential and authenticates the administrator. [3.2.1, PAM-1]
3. [FICAM and CDM] The ACS verifies that the access control privileges of the administrator match the policies, and access is granted. [3.2.2, PAM-3]
4. [FICAM] The administrator identifies the target NPE account credential in the key vault.
5. [FICAM] The administrator retrieves the target NPE's credential (including the secret) from the key vault.
6. [FICAM] The administrator generates a new secret in the security key vault system for the target NPE.
7. [FICAM] The administrator logs onto the agency Identity Store (e.g., agency AD) as the administrator and identifies the target NPE's credential.
8. [FICAM] The administrator requests the change of the secret (or password) for the target NPE's credential (in the agency AD).
9. [FICAM] The administrator updates the target NPE credential with the new secret (in the agency AD).
10. [FICAM] The administrator confirms the change and exits the agency Identity Store.
11. [CDM] The CDM system updates the desired state of the NPE status in the agency Identity Store with the renewal information.
12. [FICAM] The administrator logs onto the target application hosted on the target system.
13. [FICAM] The administrator updates the NPE's credential for the target application with the new secret.
14. [FICAM] The administrator exits the target system.
15. [CDM] The CDM system updates the desired state of the NPE for the target application to include the secret renewal information.
16. [FICAM] The administrator updates the NPE credential with the new secret in the key vault system.
17. [CDM] The CDM system updates the desired state of the NPE credential in the agency security key vault system to include the secrets renewal information.

Post-condition: The NPE's credential is updated in all systems. Note that this process can be automated to support scheduled routine password rotation. This will be captured by CDM in the proposed PRIV-REV and CRED-SFA metrics, see Section 6.4. CDM monitors these steps as indicated, and reports deviations from the expected states.

6.3.6.3 Regular User Access to Cloud Application through SP-initiated SSO Use Case

A use case is provided to describe the user (non-administrator) access, via SSO, to cloud applications and is service provider initiated upon a user's access request. Note that this is for regular users and not privileged users.

FICAM Reference: Motivated by FICAM architecture Use Case 8, "Accept Federation Assertions."[58]
Description: User access to an agency application hosted in the cloud.
Actors: Agency user, existing PIV credential, agency IdP (e.g., AD with Federated SSO service), Target Cloud Service, Target System
Pre-condition: The agency cloud application is configured to support federated user authentication. A trust relationship has been established between the two parties: the IdP and the Service Provider. The federation service within the IdP supports SAML-based SSO for user authentication.
Steps with Data Flow (These correspond with the numbered flows in Figure 6-6):

1. [FICAM] An agency user initiates a request to access a cloud application hosted by the CSP.
2. [FICAM] The cloud application forwards the incoming request to the federation service for access control decision.
3. [FICAM] The federation service at the Service Provider sends a Hypertext Markup Language (HTML) form back to the user's browser with a SAML request for user authentication.
4. [FICAM] The user's browser is redirected to the SSO service and posts the SAML authentication request.
5. [FICAM] The federated SSO service authenticates the user with the user's PIV card. Additional user attributes and claims may be retrieved from the user identity or attribute data store (such as AD) for inclusion in the SAML response.
6. [FICAM] The SSO service at the IdP returns an HTML form to the browser with a signed SAML response containing the authentication assertion with any additional attributes and claims.
7. [FICAM] Upon receipt of the user's authentication assertion with the attributes and claims, the user's browser posts the SAML response to the Service Provider for authorization.
8. [FICAM] The federation service at the Service Provider evaluates the user's identity and attributes and claims in the SAML response and authorizes access. The Service Provider establishes a session for the user and redirects the user's browser to the target resource.

Figure 6-7 provides a top-level view of how CDM services trace to Access Management functions and interact with cloud services.

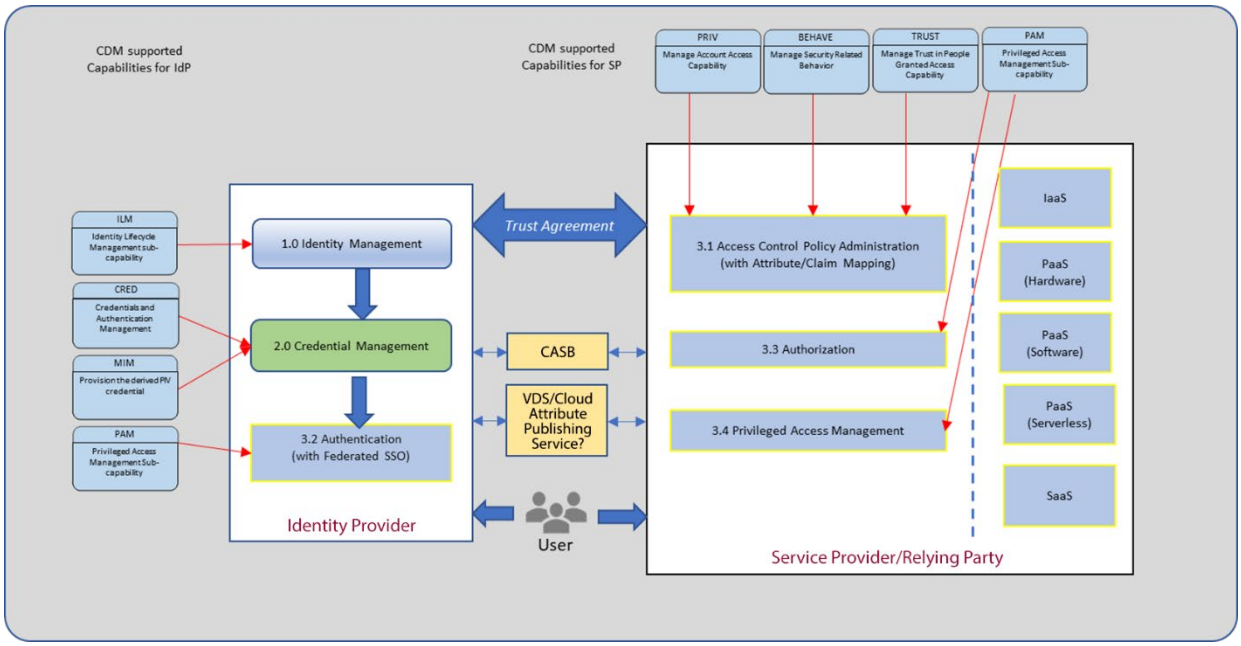


Figure 6-7: Top-Level CDM ICAM Representation With Cloud Services

[58] General Services Administration. "The Federal Identity, Credential, and Access Management Architecture," Version 3.1, FINAL. January 6, 2021, accessed May 20, 2022. https://playbooks.idmanagement.gov/docs/ficam-arch.pdf. https://playbooks.idmanagement.gov/docs/ficam-arch.pdf

6.4 CDM ICAM REFERENCE ARCHITECTURE DATA AND METRICS

CDM collects agency-defined desired-state policies for TRUST, BEHAVE, CRED, and PRIV in machine-readable form from authoritative sources. It collects actual-state IDAM data from authoritative sources for comparison with the desired state. IDAM reports the actual state and defects to agency dashboards via the MUR. Table 6-1 provides a summary of the actual-state data collected (similar desired-state data are also collected) and output (either stored in the MUR and reported to the Agency Dashboard or captured locally in logs) for each IDAM capability. MIM, ILM, and PAM data needs are also described in the table. Refer to the CDM Data Model for actual data requirements.

Table 6-1: CDM IDAM Capability Data

Capability	Collected Data (Input)	Output
TRUST	Data associated with trust in people granted access (background investigations, suitability, non-disclosure agreements, etc.), desired-state data	Actual state, defects (expired trust, etc.), logs
BEHAVE	Security-related behavior data (training, user agreements, etc.), desired-state data	Actual state, defects (required training not completed, etc.), logs
CRED	Credential and authentication data (user identification, credential type, status, etc.), desired state data, user status (includes NPE), user type (includes NPE)	Actual state, defects (account revoked or suspended due to CRED, etc.), logs
MIM	PIV certificates, PIV-D certificates, desired-state data	Request for derived PIV, certificate payloads, credential revocations, logs
PRIV	Privilege information (privilege type, review status, etc.), desired-state data	Actual state, defects (expired privileges, etc.), logs
ILM	Privileged user data: TRUST, BEHAVE, and CRED attributes; privilege review status, desired-state data	Privileged user data changes, provisioning actions, review notifications, responsibility delegation, logs (workflow events)
PAM	PIV-based strong authenticator; TRUST, BEHAVE, and CRED attributes; privileged accounts on network, desired-state data	Prompts for reviews, authentication decisions, access decisions, logs

The CDM metrics development process is based on threat techniques and mitigations. The basis is MITRE's Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) Matrix for Enterprise, a knowledgebase of adversary tactics and techniques. Other CISA programs [e.g., .gov Cybersecurity Architecture Review (.govCAR)] are also evaluating ATT&CK as a paradigm for mapping threat techniques, mitigations, and other aspects of cybersecurity.

The CDM metrics development process consists of the following steps:

1. Associate threat mitigations with CDM capabilities.
2. Identify applicable threat techniques for mitigations associated with CDM capabilities.
3. Identify currently required CDM metrics for the capabilities.
4. Identify proposed new metrics for the capabilities.
5. Determine metric data and scoring for new metrics.
6. Associate capability area metrics with NIST Cybersecurity Framework and NIST SP 800-53.
7. Document the metrics.

Table 6-2 shows currently required metrics in CDM.

Table 6-2: Currently Required Metrics

Metric	Name
TRUST-EXP	Expired TRUST
BEHAVE-RTNC	Required Training Not Completed
BEHAVE-EXP	Expired Training
CRED-EXP	Expired CRED

Metric	Name
CRED-ACCOUNT	CRED Review Not Completed
CRED-ARAA	Accounts Revoked or Suspended Due to CRED

Table 6-3 shows near-term proposed CDM metrics; Table 6-4 shows more future-looking metrics.

Table 6-3: Proposed Metrics

Metrics	Name
TRUST-FAIL	Account Revoked
CRED-SFA	MFA Not Used or Required
PRIV-REV	Account with Privileges Not Reviewed Within the Last 90 Days

Table 6-4: Future Metrics

Metric	Name
CRED-AUTHN	Failure to Secure Authentication
CRED-COMP	Failure to Secure Credentials
PRIV-ESC	Failure to Monitor for Privilege Escalation
BEHAVE-CONT	Failure to Train with Approved Materials
PRIV-PEX	Expired Trust
PRIV-LEAST	Privileged Account

7. PHYSICAL SOLUTION ARCHITECTURE

7.1 CURRENT ARCHITECTURE

A notional CDM ICAM physical architecture is shown in Figure 7-1. The TRUST, CRED, BEHAVE, and PRIV information is integrated into the MUR by SailPoint IdentityIQ at Layer A. The MUR data is provided through the integration layer (Layer B) implemented by Splunk, RedHat, or AXONIUS to the Agency Dashboard (Layer C). The Agency Dashboard (Elastic) feeds summarized data to the Federal Dashboard (Elastic). CyberArk or CA Technologies implements the PAM and ILM functions, interacting with IdentityIQ.

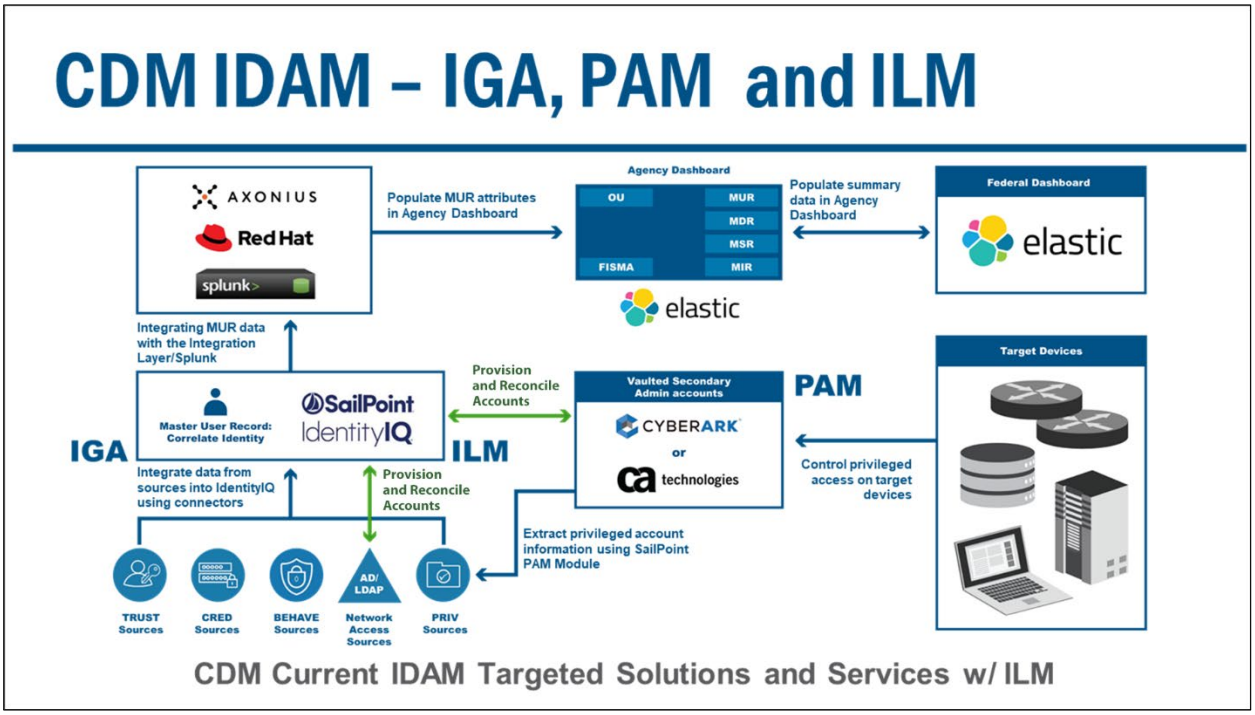


Figure 7-1: Example Physical Architecture

7.2 POTENTIAL FUTURE ARCHITECTURE

Figure 7-2 depicts the logical architecture of NIST NCCOE Zero Trust Enhanced Identity Governance (EIG) Enterprise Build 1 (E1B1).[59] EIG E1B1 uses products from Amazon Web Services, IBM, Ivanti, Mandiant, Okta, Radiant Logic, SailPoint, Tenable, and Zimperium. Certificates from DigiCert are also used.

E1B1 was designed with a single ICAM system (Okta Identity Cloud) that serves as the identity, access, and credential manager as well as the ZTA PE and PA. It includes the Ivanti Sentry as its PEP, and it also delegates some PDP responsibilities to Ivanti Access ZSO (Zero Sign-On). Radiant Logic acts as a PIP for the PDP because it responds to inquiries and provides identity information on demand in order for Okta to make near-real-time access decisions.

[59] National Institute of Standards and Technology (NIST), "Implementing a Zero Trust Architecture Volume B: Approach, Architecture, and Security Characteristics, NIST SP 1800-35B" (Second Preliminary Draft), December 21, 2022, https://www.nccoe.nist.gov/sites/default/files/2022-12/zta-nist-sp-1800-35b-preliminary-draft-2.pdf.

2378 Figure D-1 Logical Architecture of E1B1

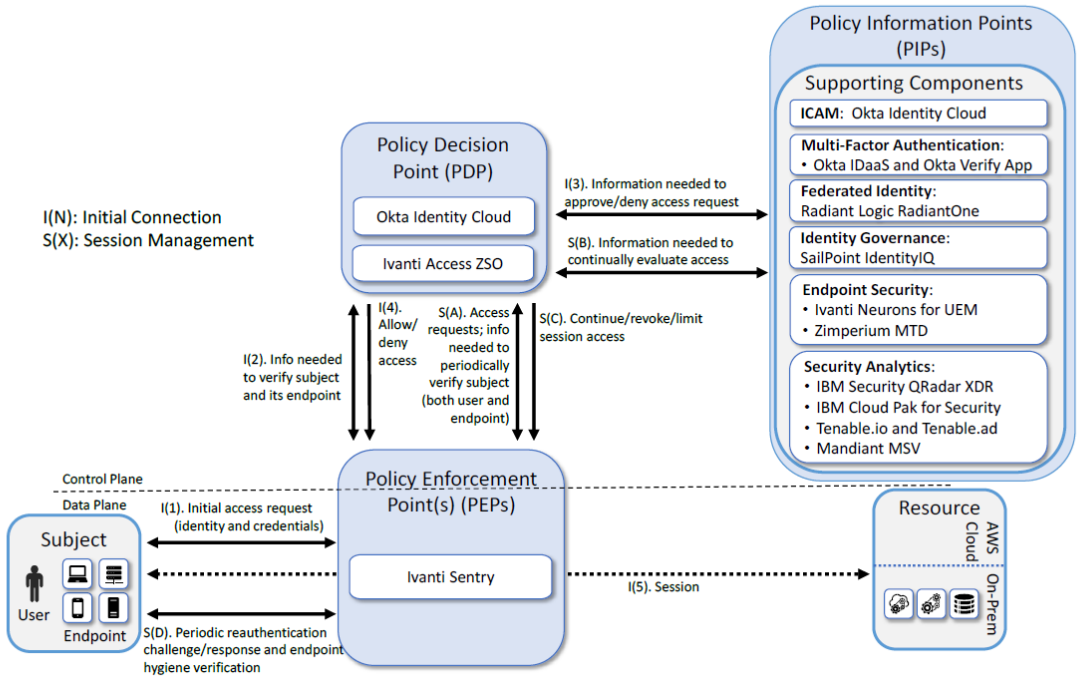


Figure 7-2: Logical Architecture of Zero Trust (From NIST SP 1800-35B)

Figure 7-3 shows CDM-supported capabilities related to the Zero Trust E1B1 ICAM Information Architecture – Identity Correlation implementation components. The PAM function has not been addressed to date but will need to be in the future. Some agencies have implemented some of these capabilities.

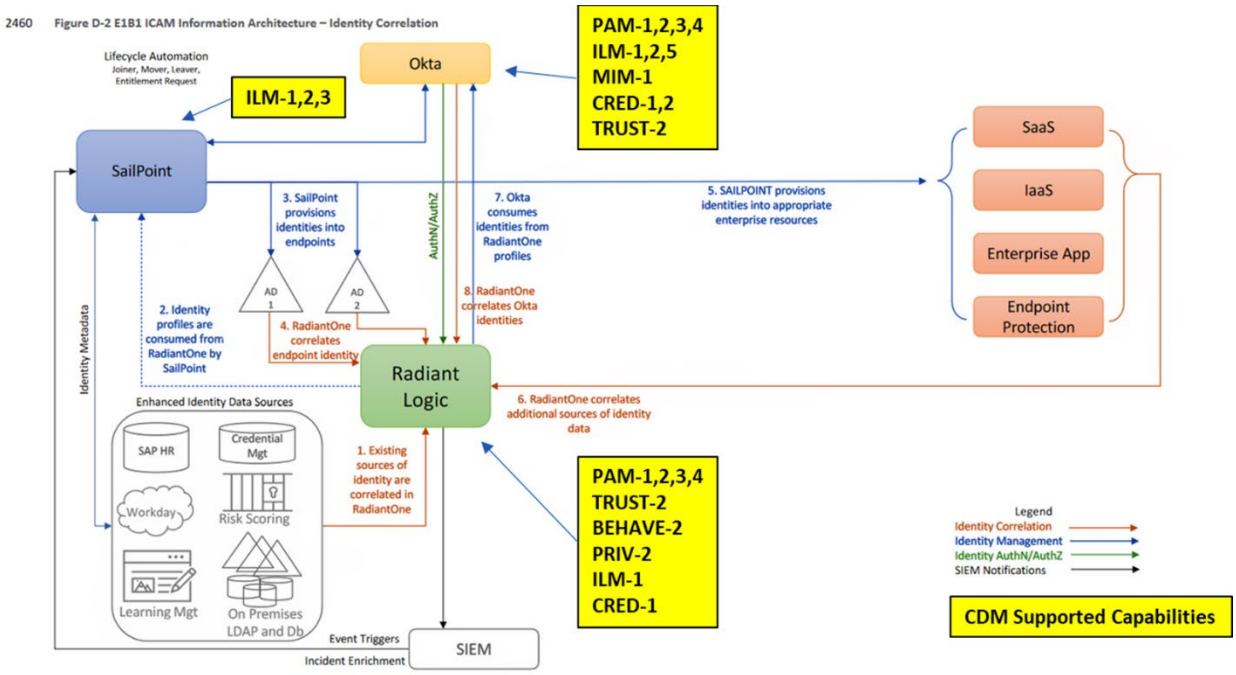


Figure 7-3: CDM Functions Mapped to Zero Trust ICAM Information Architecture (From NIST SP 1800-35B)

8. CDM AND FICAM CHALLENGES

The following challenges exist for CDM ICAM:

- Funding for CDM capabilities is not consistent across all of the Federal Civilian Executive Branch (FCEB) and therefore some elements of CDM may be deployed at one agency and not at another agency.
- Agencies use various systems for ICAM, so there is not a "standard" CDM ICAM physical architecture.
- Agencies' authoritative sources of information upon which CDM relies differ in a variety of formats, making it a challenge to define CDM ICAM data requirements that apply across all agencies.
- There are issues identifying and gaining access to authoritative sources of data and level of content (e.g., BEHAVE, grace periods) and CDM-specified data elements.
- CDM logical data model and CDM dashboard implementation are not always consistent.
- Government policy changes over time and can differ by agency. While CDM endeavors to align with policies, the primary function of CDM is to help agencies identify and reduce risk to their environment.
- Zero Trust implementations are immature and still evolving so CDM ICAM will need to keep pace. Standards are particularly missing:
    - A standard that supports Zero Trust metadata labeling is needed to appropriately tag stored data, to allow fine-grained restriction policies and enforcement. This does not currently exist.
    - A standard that supports automated response, such as Security Orchestration, Automation, and Response, is not available to provide the fine-grained remediation actions necessary for ZTA. Therefore, until such a standard is developed, there will be no support for automation interoperability between vendor products.

CDM continues to evolve the CDM data model such that it incorporates data elements that can reasonably be expected to be provided by agency authoritative sources while allowing for variations in that supplied data.

9. CONCLUSION

There is no singular, authoritative, recognized way to architect an ICAM capability across an enterprise, particularly as enterprises extend to the cloud. U.S. government agencies approach ICAM from different perspectives given their size, sensitivity of information, complexity, and implementation across legacy and cloud environments. The federal government is benefited by the existence of a high-level federal ICAM architecture, and this reference takes advantage of that model. This reference architecture is developed to further refine the FICAM architecture and highlights specific functions of that architecture that the CDM Program relies on as a functional base. The FICAM reference described here will support specific use cases that CDM considers fundamental.

When describing use cases, we show the functions that are identified within FICAM services and associated playbooks, the functions that are described in CDM requirements, or both, as applicable. The intended audience of this document is CDM stakeholders interested in CDM ICAM capabilities and how they might be integrated with agency FICAM components.

Three CDM capability areas were identified to represent FICAM practice areas: Identity Management is primarily represented in TRUST, Credential Management is primarily represented in CRED, and Access Management is primarily represented in BEHAVE and PRIV. Within each capability, assumptions and constraints, functions, and illustrative use cases to describe actors and their intended steps are provided. Governance and federation capabilities are also considered. Applicable CDM IDAM capability data and metrics that may be applicable to this reference architecture are identified. This document does not cover the details of a physical interface between CDM and other FICAM components because that can differ across agencies. It does, however, provide a high-level, notional physical implementation. Some challenges associated with integrating CDM, and agency FICAM functions are described.

Enterprise architectures are evolving to incorporate Zero Trust as a central, guiding principle for constructing modern, secure integrated system architectures. This release of the CDM FICAM Reference Architecture addresses specific requirements of ZTA and illustrates how ICAM and CDM help enable it.

CDM capability areas for Access management are addressed for PEs, NPEs and Privileged users, but SSO and digital worker identities will need to be addressed as well since they are rapidly being implemented. CDM threat management assumes agencies use Active Directories that are leveraged for SSO on-premises using Kerberos, which is insufficient for Zero Trust architectures.

For SSO, the Cloud Identity Playbook states IDaaS can incorporate it along with MFA and directory services in a single platform that supports multiple phishing-resistant authenticator options. IDaaS is a common cloud identity model that the CDM Program expects to be addressing soon.

For digital identity workers, there is a lack of Zero Trust capability that should be added. Profiles of federated authentication protocols are essential for interoperability at known assurance levels within enterprises. The ILM playbook[60] discusses a shift in managing credentials to managing identities.

The CDM model focuses on system boundaries based on FISMA system-based identification, but the workflow and application tier of Zero Trust does not align well with the currently designated FISMA model.

[60] General Services Administration, "Identity Lifecycle Management Playbook," Version 1.2, December 15, 2022, https://playbooks.idmanagement.gov/playbooks/ilm/.

10. NEXT STEPS

Recognizing that there are competing interests and responsibilities of the CDM Program, the following actions are next steps in developing the Identity Pillar of a Zero Trust Architecture:

1. For CFO-Act agencies, continue to provide PAM and ILM capabilities to those that have not implemented them.
2. Make updates to the CDM data model that enables querying of defects in alignment with federal CIO metrics.
3. Expand CDM requirements to address Access Management capabilities that incorporate modern single sign-on in cloud, hybrid and zero trust environments.
4. For non-CFO Act agencies, implement an Identity as a Service capability that will provide lightweight Identity Governance and robust Single-Sign On services. This will enable these agencies to better manage their users while taking advantage of modern authentication protocols offered by IDaaS Service Providers.

Encourage federal enterprise Service Providers to enable their service capabilities to integrate with CDM IDAM services for Identity Proofing, PIV Issuance and Continuous Vetting to allow better consistency and visibility into these essential functions.

APPENDIX A: BIBLIOGRAPHY

Cybersecurity and Infrastructure Security Agency. "Secure Cloud Business Applications (SCuBA) Technical Reference Architecture (TRA)." April 2022. Request for Comment Draft, accessed July 25, 2023. https://www.cisa.gov/sites/default/files/2023-06/CSSO-SCUBA-TRA-guidance%20documentV2_508c.pdf.

Cybersecurity and Infrastructure Agency. "Trusted Internet Connections 3.0." Version 1.0. June 2022. https://www.cisa.gov/sites/default/files/publications/CISA%20TIC%203.0%20Cloud%20Use%20Case%20Draft_1.pdf.

Cybersecurity and Infrastructure Security Agency. "Zero Trust Maturity Model." Version 2.0. April 2023. Accessed July 25, 2023. https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf.

Committee on National Security Systems. CNSS 4009, "Committee on National Security Systems (CNSS) Glossary." April 6, 2015.

Department of Defense. "DoD Enterprise Identity, Credential, and Access Management (ICAM) Reference Design." Version 1.0. June 2020. Accessed July 25, 2023. https://dodcio.defense.gov/Portals/0/Documents/Cyber/DoD_Enterprise_ICAM_Reference_Design.pdf.

Department of Defense. "Zero Trust Reference Architecture." Version 2.0. September 2022. Accessed July 25, 2023. https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf.

Department of Homeland Security. "CDM Data Model Document." Version 4.4.1. July 2023.

Department of Homeland Security. "Continuous Diagnostics and Mitigation (CDM) Program Cloud Guidance Document, Volume 1, Architecture, Data Flows, and Data Sources." Version 2.0. May 2020.

Department of Homeland Security. "Continuous Diagnostics and Mitigation (CDM) Program Cloud Guidance Document, Volume 2, Cloud-Service Support for CDM." Version 2.0. May 2020.

Department of Homeland Security. "Continuous Diagnostics and Mitigation (CDM) System Architecture: CDM Data Model Document." Version 4.0. May 2022.

Department of Homeland Security. "Continuous Diagnostics and Mitigation (CDM) Program Technical Capabilities, Volume 2: Requirements Catalog." Version 2.5, July 2023.

Department of Defense Chief Information Officer. "Policies and Priorities Identity, Credentialing, and Access Management (ICAM)." Accessed May 20, 2002. https://www.cio.gov/policies-and-priorities/ICAM/.

Executive Office of the President, Federal Chief Information Officers Council. "Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, Version 2.0." December 2, 2011. Accessed July 25, 2023. https://playbooks.idmanagement.gov/docs/roadmap-ficam.pdf.

Executive Office of the President, Office of Management and Budget. "Enabling Mission Delivery through Improved Identity, Credential, and Access Management." OMB-M-19-17. May 21, 2019. Accessed May 20, 2002. https://www.whitehouse.gov/wp-content/uploads/2019/05/M-19-17.pdf.

Executive Office of the President, Office of Management and Budget. "Moving the U.S. Government Toward Zero Trust Cybersecurity Principles," OMB-M-22-09. January 26, 2022. Accessed November 17, 2022, https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf.

Executive Order 13681, "Improving the Security of Consumer Financial Transactions." October 17, 2014, accessed July 25, 2023, https://obamawhitehouse.archives.gov/the-press-office/2014/10/17/executive-order-improving-security-consumer-financial-transactions.

Executive Order 14028, "Improving the Nation's Cybersecurity." May 12, 2021. Accessed July 25, 2023, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity.

FIPS 201-3, "Personal Identity Verification (PIV) of Federal Employees and Contractors," NIST, January 2022. Accessed April 5, 2022, https://csrc.nist.gov/publications/detail/fips/201/3/final.

General Services Administration. "Identity, Credential, and Access Management Governance Framework Appendix C: ICAM and Zero Trust." Version 1.0. September 2021. Accessed November 17, 2022. https://playbooks.idmanagement.gov/docs/playbook-identity-governance-framework.pdf.

General Services Administration. "Identity Lifecycle Management Playbook." Version 1.2. December 15, 2002. https://playbooks.idmanagement.gov/playbooks/ilm/.

General Services Administration. "Cloud Identity Playbook," Version 1.0. January 20, 2022. Accessed May 20, 2022. https://playbooks.idmanagement.gov/playbooks/cloud/.

General Services Administration. "Digital Worker Identity Playbook." Version 1.1. January 5, 2021. Accessed December 8, 2022. https://playbooks.idmanagement.gov/playbooks/dw/.

General Services Administration. "Enterprise Single Sign-On Playbook." Version 1.1. February 12, 2021. Accessed December 8, 2022. https://playbooks.idmanagement.gov/playbooks/sso/.

General Services Administration. "The Federal Identity, Credential, and Access Management Architecture." Version 3.1, FINAL. January 6, 2021. Accessed May 20, 2022. https://playbooks.idmanagement.gov/docs/ficam-arch.pdf.

Department of Homeland Security. "Policy for a Common Identification Standard for Federal Employees and Contractors, HSPD-12." August 27, 2004. Updated January 27, 2022. https://www.dhs.gov/homeland-security-presidential-directive-12.

Internet Engineering Task Force (IETF). "The OAuth 2.0 Authorization Framework: Bearer Token Usage, IETF RFC 6750." October 2012, https://datatracker.ietf.org/doc/html/rfc6750.html.

National Institute of Standards and Technology (NIST) Computer Security Resource Center (CSRC). "Glossary." March 28, 2023. https://csrc.nist.gov/glossary,

National Institute of Standards and Technology (NIST). "An Introduction Information Security, NIST SP 800-12, Revision 1." June 2017. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf.

National Institute of Standards and Technology (NIST). "Information Security Continuous Monitoring (ISCM) for Federal Information Systems, NIST SP 800-137." September 2011. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.pdf.

National Institute of Standards and Technology (NIST). "The NIST Definition of Cloud Computing, NIST SP 800-145." September 2011. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.

National Institute of Standards and Technology (NIST). "Guide to Attribute Based Access Control (ABAC) Definition and Considerations, NIST SP 800-162." January 2014. Updated August 2, 2019. https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-162.pdf.

National Institute of Standards and Technology (NIST). "Introduction to Public Key Technology and the Federal PKI Infrastructure, NIST SP 800-32." February 26, 2001. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-32.pdf. Publication withdrawn in its entirety on September 13, 2021.

National Institute of Standards and Technology (NIST). "Security and Privacy Controls for Information Systems and Organizations, NIST SP 800-53, Revision 5." September 2020. Updated December 10, 2020. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

National Institute of Standards and Technology (NIST). "Digital Identity Guidelines, NIST SP 800-63-4." December 16, 2022. Accessed July 25, 2023. https://csrc.nist.gov/pubs/sp/800/63/4/ipd.

National Institute of Standards and Technology (NIST). "Digital Identity Guidelines: Enrollment and Identity Proofing, NIST SP 800-63A." June 2017. Updated March 2, 2020. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63a.pdf.

National Institute of Standards and Technology (NIST). "Digital Identity Guidelines: Authentication and Lifecycle Management, NIST SP 800-63B." June 2017. Updated March 2, 2020. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf.

National Institute of Standards and Technology (NIST). "Digital Identity Guidelines: Federation and Assertions, NIST SP 800-63C." June 2017. Updated March 2, 2020. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63c.pdf.

National Institute of Standards and Technology (NIST). "Zero Trust Architecture, NIST SP 800-207." August 2020. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf.

National Institute of Standards and Technology (NIST). "Implementing a Zero Trust Architecture Volume A: Executive Summary, NIST SP 1800-35A." Second Preliminary Draft. December 21, 2022. https://www.nccoe.nist.gov/sites/default/files/2022-12/zta-nist-sp-1800-35a-preliminary-draft-2.pdf

National Institute of Standards and Technology (NIST). "Implementing a Zero Trust Architecture Volume B: Approach, Architecture, and Security Characteristics, NIST SP 1800-35B." Second Preliminary Draft. December 21, 2022. https://www.nccoe.nist.gov/sites/default/files/2022-12/zta-nist-sp-1800-35b-preliminary-draft-2.pdf.

National Institute of Standards and Technology (NIST). "Implementing a Zero Trust Architecture Volume C: How-To Guides, NIST SP 1800-35C." Second Preliminary Draft. December 21, 2022. https://www.nccoe.nist.gov/sites/default/files/2022-12/zta-nist-sp-1800-35c-preliminary-draft-2.pdf.

National Institute of Standards and Technology (NIST). "Implementing a Zero Trust Architecture Volume D: Functional Demonstrations, NIST SP 1800-35D." Second Preliminary Draft. December 21, 2022. https://www.nccoe.nist.gov/sites/default/files/2022-12/zta-nist-sp-1800-35d-preliminary-draft-2.pdf.

National Security Agency. "Embracing a Zero Trust Security Model." Version 1.0. February 2021. https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF.

APPENDIX B: GLOSSARY AS APPLIED TO FICAM

Assertion – A statement from a verifier to a relying party that contains information about a subscriber (e.g., for the purpose of subscriber validation). Assertions may contain verified attributes (e.g., for authentication and authorization). (Source: NIST SP 800-63-3)

Authenticator – Something the claimant possesses and controls (typically a cryptographic module or password) that is used to authenticate the claimant's identity. In previous versions of NIST SP 800-63-3, this was referred to as a token. Clarification of scope: The means used to confirm the identity of a user, process, or device (e.g., user password or token). (Source: CNSSI 4009)

Authenticator Output – The output value generated by an authenticator. The ability to generate valid authenticator outputs on demand proves that the claimant possesses and controls the authenticator. Protocol messages sent to the verifier are dependent on the authenticator output, but they may or may not explicitly contain it. (Source: NIST SP 800-63-3)

Bearer Assertion – The assertion a party presents as proof of identity, where possession of the assertion itself is sufficient proof of identity for the assertion bearer. (Source: NIST SP 800-63-3) Also known as Bearer Token, as defined in IETF Request for Comment (RFC) 6750.

Binding – A created, and subsequently established, association between an identity and an authenticator. (Source: NIST SP 800-63-3, clarified)

Certificate – A digital certificate, also known as a PK certificate, is used to cryptographically link ownership and authority of a PK with the entities that either own or issue the certificate, respectively. Digital certificates are used to share public keys for encryption and authentication purposes. (Source: CDM Integrated Data Dictionary, AV-2.) This digital representation of information, at a minimum: (1) identifies the CA issuing it; (2) names or identifies its subscriber; (3) contains the subscriber's PK; (4) identifies its operational period; and (5) is digitally signed by the CA issuing it. (Source: NIST SP 800-32)

Mobile Device – A portable computing device that has a small form factor so that it can easily be carried by a single individual; is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); possesses local, non-removable data storage; and is powered on for extended periods of time with a self-contained power source. Mobile devices may also include voice communication capabilities and onboard sensors that allow the device to capture, for example, photographs and video.

Non-Person Entity – An NPE is an autonomous service, application, or device that may be granted a CRED to accomplish a necessary function within an agency. An NPE can be used to facilitate documenting an account that is intended to be used by a system or application (i.e., service account) to either accomplish some necessary function or provide a group service that does not require a person(s) to actively manage or login to use, such as a group mailbox.

Relying Party – A relying party is a service that requires an IdP to provide authentication. The relying party is usually an application or a cloud service, and it contains subscriber information (usually a username.) It may also have additional attributes such as the authenticator type used in the access control decision. (Source: Derived from "Cloud Identity Playbook," January 2022, Version 1.0)

Token – See Authenticator.

APPENDIX C: ACRONYMS

.govCAR	.gov Cybersecurity Architecture Review
AAL	Authenticator Assurance Level
AAS	Authoritative Attribute Service
ABAC	Attribute-Based Access Control
ACS	Access Control System
AD	Active Directory
ADFS	AD With Federated SSO Service
AEC	Application Execution Control
AI	Artificial Intelligence
AM	Asset Management
ATT&CK®	Adversarial Tactics, Techniques, and Common Knowledge
AUTH	Authenticated
BEHAVE	Manage Security-Related Behavior
BOUND	Boundary Protection
BR	Backup and Recovery
CA	Certification Authority
CASB	Cloud Access Security Broker
CDM	Continuous Diagnostics and Mitigation
C-DPM	Cloud Data Protection Management
CFO	Chief Financial Officer
C-IAM	Cloud Identity and Asset Management
CIO	Chief Information Officer
CISA	Cybersecurity and Infrastructure Security Agency
CMS	Credential Management System
C-NSM	Cloud Network Security Management

CNSSI	Committee on National Security Systems Instruction
CRED	Manage Credentials and Authentication
CSACS	Cloud Service Access Control System
CSM	Configuration Settings Management
CSP	Cloud Service Provider
CSPM	Cloud Security Posture Management
CSR	Certificate Signing Request
CVM	Configuration and Vulnerability Management
DHS	Department of Homeland Security
DNS	Domain Name System
DPC	Derived Personal Identity Verification Credentials
E1B1	EIG Enterprise Build 1
EDR	Endpoint Detection and Response
EIG	Enhanced Identity Governance
EMM	Enterprise Mobility Management
EO	Executive Order
EPP	Endpoint Protection Platform
FAL	Federation Assurance Level
FICAM	Federal Identity, Credential, and Access Management
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
GS	Governance Strategy
GSA	General Services Administration
HSPD	Homeland Security Presidential Directive
HTML	Hypertext Markup Language
HWAM	Hardware Asset Management
IaaS	Infrastructure as a Service

IAL	Identity Assurance Level
ICAM	Identity, Credential, and Access Management
IDaaS	Identity as a Service
IDAM	Identity and Access Management
IDMS	Identity Management System
IdP	Identity Provider
IETF	Internet Engineering Task Force
IGA	Identity Governance and Administration
ILM	Identity Lifecycle Management
IM	Identity Management
iOS	Apple Operating System
IoT	Internet of Things
IP	Internet Protocol
ISCM	Information Security Continuous Monitoring
IT	Information Technology
JHU/APL	The Johns Hopkins University Applied Physics Laboratory
LDAP	Lightweight Directory Access Protocol
LT	Logging and Threats
MDM	Master Data Management
MDR	Master Device Record
MFA	Multi-Factor Authentication
MIM	Mobile Identity Management
MIR	Master Incident Record
MNGEVT	Manage Events
MSR	Master System Record
MUR	Master User Record
NAC	Network Access Control

NIST	National Institute of Standards and Technology
NPE	Non-Person Entity
NS	Network Security
OIDC	OpenID Connect
OMB	Office of Management and Budget
OMI	Operate, Monitor, and Improve
OU	Organizational Unit
PA	Policy Administrator
PaaS	Platform as a Service
PAM	Privileged Access Management
PDP	Policy Decision Point
PE	Person Entity
PE	Policy Engine
PEP	Policy Enforcement Point
PII	Personally Identifiable Information
PIN	Personal Identification Number
PIP	Policy Information Point
PIV	Personal Identity Verification
PIV-D	Derived PIV
PK	Public Key
PKI	Public Key Infrastructure
PMO	Program Management Office
PRIV	Privilege Management
PROT	Protection Management
RBAC	Role-Based Access Control
RFC	Request for Comment
SaaS	Software as a Service

SAML	Security Assertion Markup Language
SCuBA	Secure Cloud Business Applications
SIEM	Security Information and Event Management
SP	Special Publication
SPIL	Data Breach/Spillage Mitigation
SSO	Single Sign-On
SWAM	Software Asset Management
TRA	Technical Reference Architecture
TRUST	Manage Trust in People Granted Access
VUL	Manage Vulnerabilities
ZTA	Zero Trust Architecture