

Digital Policy Management Framework for Attribute-Based Access Control

Contract Milestone Task 12.1

19 December 2014

The Johns Hopkins University Applied Physics Laboratory

Table of Contents

- Executive Summaryiv
- 1 Introduction 1
 - 1.1 Purpose..... 1
 - 1.2 Intended Audience and Use 1
 - 1.3 Scope..... 2
 - 1.4 Applicability 2
 - 1.5 Document Organization 3
- 2 ABAC and DPM Background..... 4
 - 2.1 ABAC Concepts..... 4
 - 2.2 DPM Background..... 9
- 3 DPM Capability Needs and Requirements..... 13
 - 3.1 DPM Capability Needs 13
 - 3.2 DPM Requirements 14
- 4 DPM Reference Architecture 28
 - 4.1 DPM RA Overview 28
 - 4.2 DPM Functional Components 28
 - 4.3 Use Case Realization in the DPM RA 30
- 5 DPM Implementation Considerations..... 39
 - 5.1 Protection of DP..... 39
 - 5.2 DP in an Information Sharing Environment 39
 - 5.3 Importance of the Context Handler 40
 - 5.4 Human-Readable Structured Language Policy 41
 - 5.5 DP Feedback and Override..... 43
 - 5.6 Caching Assertions 44
- 6 DPM RA Technology and Standards Overlay..... 45
 - 6.1 Current and Planned Technologies and Standards 45
 - 6.2 Implementation Recommendations 46
- A References A-1
- B Acronyms B-1
- C Glossary C-1

List of Illustrations

Figure 1: Basic ABAC Model.....	5
Figure 2: Decomposition of the ACM.....	5
Figure 3: DPM Functional Overview	11
Figure 4: DPM Use Case Actors	16
Figure 5: DPM for ABAC Use Case Diagram.....	17
Figure 6: DPM RA Functional Components.....	30
Figure 7: Sequence Diagram for Manage DP Content Use Case	31
Figure 8: Sequence Diagram for Approve DP Content Use Case	32
Figure 9: Sequence Diagram for Evaluate and Deconflict DPs Use Case	33
Figure 10: Sequence Diagram for Manage Activated DPs Use Case	34
Figure 11: Sequence Diagram for Enforce DPs Use Case	35
Figure 12: Sequence Diagram for Monitor DP Enforcement Use Case	36
Figure 13: Sequence Diagram for Import and Export Policies Use Case	36

List of Tables

Table 1: DPM Framework Audience and Use	2
Table 2: DPM Capability Descriptions.....	13
Table 3: Use Case Description Format.....	17
Table 4: Manage DP Content Use Case Description	18
Table 5: Approve DP Content Use Case Description	20
Table 6: Evaluate and Deconflict DPs Use Case Description	21
Table 7: Manage Activated DPs Use Case Description	22
Table 8: Enforce DPs Use Case Description	25
Table 9: Monitor DP Enforcement Use Case Description	26
Table 10: Import and Export Policies Use Case Description	27
Table 11: HRSLP Policy and Context Information.....	41
Table 12: Recommended Structure for HRSLP Rules	42

Executive Summary

The Digital Policy Management (DPM) Framework for Attribute-Based Access Control (ABAC), herein called the DPM Framework, provides a conceptual structure intended to serve as a guide for developing systems, standards, and technologies that implement DPM functions for ABAC policies. That conceptual structure includes DPM terminology, requirements, reference architecture (RA), and implementation considerations.

The DPM Framework is offered as proposed content that extends the Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance to include DPM functions for ABAC policies.

The scope of this document is limited to functions that manage digital policy (DP) for controlling access to protected resources and appropriate information sharing across the Federal Enterprise. This includes DPs with Federal, agency, and organizational scope within hierarchical relationships and DPs derived from peer-to-peer information sharing agreements.

The terms and definitions used herein are aligned to the maximum extent possible with the Identity, Credential, and Access Management Capabilities Lexicon. Many of the concepts described in this document are directly based on National Institute of Standards and Technology (NIST) Special Publication (SP) 800-162 and the ABAC reference model used in the eXtensible Access Control Markup Language (XACML) standards (e.g., XACML 3.0). Familiarity with those documents is assumed.

There are viable products that perform many of the Enterprise DPM functions. Most of the DPM-capable products are part of a suite that includes policy decision and enforcement, and most support XACML as the policy language. Use of the XACML standard suggests that a heterogeneous mix of these products could be used to implement policy decision points (PDPs) and policy enforcement points (PEPs), while choosing a smaller subset for the DPM functionality. Few of these products allow the separation of PDP and PEP, and most employ some form of proprietary interface between PDP and PEP.

One major gap in DPM functionality for these products is the automated support for translation of Natural Language Policies (NLPs) and business rules into DP. The absence of this function is an indicator of the difficulty in performing the automated translation. Capturing the intent of NLPs and business rules requires knowledge of the mission or business domain terminology; therefore, a trial-and-error approach with correction based on user feedback is required.

Only a few products support auditing and monitoring of the operational effects of either changing DPs or delaying the dissemination of those changes. It is not clear whether those products could be used to monitor the effects for policies generated and disseminated by products from other vendors.

The following implementation recommendations are provided for consideration by the FICAM community:

Recommendation 1: Review, revise, and approve the DPM RA.

This should include:

- Coordinating this document with departments and agencies and interdepartmental working groups.
- Updating FICAM Roadmap and Implementation Guidance documents to reflect the approved DPM RA.

Recommendation 2: Establish best practices for approval of Human-Readable Structured Language Policy (HRSLP) and DP.

This should include:

- Establishing a standard format for HRSLP.
- Using a risk-driven approach for defining the evidence required for approval.

Recommendation 3: Use the approved RA in acquisition strategy.

This should include:

- Offering this document for consideration in establishing a NIST SP that augments NIST SP 800-162 with additional DPM detail.
- Using the functional requirements to drive commercial and Government-funded development of Enterprise-wide DPM capabilities.
- Deriving criteria from the requirements for use in trade studies comparing commercial technologies.
- Identifying critical functionality that should be developed or accelerated with Government funding.

1 Introduction

1.1 Purpose

The Digital Policy Management (DPM) Framework for Attribute-Based Access Control (ABAC), herein called the DPM Framework, provides a conceptual structure intended to serve as a guide for developing systems, standards, and technologies that implement DPM functions for ABAC policies. That conceptual structure includes DPM terminology, requirements, reference architecture (RA), and implementation considerations. This is consistent with the following “framework” definition from [whatis.com](#) (Reference 1): “A real or conceptual structure intended to serve as a support or guide for the building of something useful.”

The DPM Framework is offered as proposed content that extends the Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance (Reference 2) to include DPM functions for ABAC policies.

The terms and definitions used herein are aligned to the maximum extent possible with the Identity, Credential, and Access Management Capabilities (ICAM) Lexicon (Reference 3). Many of the concepts described in this document are directly based on National Institute of Standards and Technology (NIST) Special Publication (SP) 800-162 (Reference 4) and the ABAC reference model used in the eXtensible Access Control Markup Language (XACML) standards (e.g., XACML 3.0) (Reference 1). Familiarity with those documents is assumed.

As used in this document, the term DPM encompasses the acts of dynamically creating, disseminating, and maintaining hierarchical rule sets to control digital resource management, utilization, and protection (Reference 3). These rule sets, or digital policies (DPs), express ABAC policies that are used in ACMs to determine whether a subject is authorized to access an object.

Per NIST SP 800-162, ABAC is “an access control method where subject requests to perform operations on objects are granted or denied based on assigned attributes of the subject, assigned attributes of the object, environmental conditions, and a set of policies that are specified in terms of those attributes and conditions.”

Nothing in this document should be considered prescriptive or directive in nature. Detailed design and implementation specifics should be as determined by the implementing organization. The DPM Framework merely serves as a foundation for understanding the elements needed to implement a DPM capability and the available design trade space. Mandate of this guidance or any of the design elements herein should be incorporated by reference in an appropriate and authoritative policy document for the implementing entity.

1.2 Intended Audience and Use

The primary audience of the DPM Framework is the membership of the working groups responsible for updating the FICAM Implementation Roadmap and Guidance documents. Once those

working groups have reviewed, modified, approved, and coordinated the DPM Framework to be added to the FICAM guidance, the audience is expected to include others, as shown in Table 1.

Table 1: DPM Framework Audience and Use

Audience	Document Use
All	General educational overview of DPM for ABAC.
Federal Government officials	Use the architecture and requirements to guide DPM implementation and to identify critical DPM functionality that should be developed or accelerated with Government funding.
Product developers	Use the architecture and requirements to identify opportunities to align their DPM technology offerings with Federal agencies' ICAM needs.
Product evaluators	Use the RA as a conceptual model and derive criteria from the requirements for use in trade studies comparing commercial products.
Integrators	Use the RA as a conceptual model for allocating requirements to vendor products.
Standards bodies	Use the architecture and requirements to identify opportunities to establish or improve applicable standards.

1.3 Scope

The scope of this document is limited to functions that manage DP for controlling access to protected resources and appropriate information sharing across the Federal Enterprise. This includes DPs with Federal, agency, and organizational scope within hierarchical relationships and DPs derived from peer-to-peer information sharing agreements.

Many of the functions could be used to manage access control policies of local organizations, but the proposed content focuses on enterprise management of DPs with hierarchical or peer-to-peer implications. The functions could also apply to management of other types of DPs (e.g., security configuration, physical access, and information flow control), but this document does not assess the applicability of the functions to those policy types, nor does it address DPM considerations that would be unique to those types.

1.4 Applicability

The DPM Framework is applicable to U.S. Government Federal departments and agencies (D/As). Committee for National Security Systems Directive (CNSSD) 507, *National Directive for Identity, Credential, and Access Management (ICAM) Capabilities on the United States Federal Secret Fabric* (Reference 5), directs Federal D/As to implement ABAC capabilities for the protection of shared information on the Federal Secret Fabric and mandates the use of DPs to represent authorization rules. Similar governance is being developed to mandate ABAC and other FICAM capabilities on Unclassified and Top Secret networks as well. The DPM Framework is intended to provide high-level DPM capability design guidance and considerations to ensure interoperability and compliance with ABAC capability employment for information sharing on all network fabrics. Subsequent and specific implementation guidance will need to be developed for each fabric.

Although the DPM Framework focuses on DPM capabilities needed for Federal Enterprise inter-organization information sharing, it also provides the guidance for the attribute management and access control mechanism (ACM) deployment and functionality (beyond existing Federal guidance) that is needed to enable an end-to-end ABAC authorization capability.

1.5 Document Organization

The remainder of this document is organized as follows:

- Section 2 provides DPM background information, including explanations of terms and concepts and an overview of DPM capabilities.
- Section 3 presents DPM use cases and requirements derived from the capabilities and identifies the users and external non-person entities involved in the use cases.
- Section 4 includes the RA to guide DPM implementation and traces the use case functionality through the architecture.
- Section 5 describes implementation considerations and discusses the current and planned technologies and standards that may be candidates for DPM implementation in Federal information technology systems.
- Section 6 discusses the suitability of the current and planned technologies and standards for implementation of the DPM reference architecture.
- Appendix A lists the cited references.
- Appendix B defines the acronyms used herein.
- Appendix C defines key terms.

2 ABAC and DPM Background

The terms and definitions used herein are aligned to the maximum extent possible with the ICAM Lexicon (Reference 3). Many of the concepts described in this document are directly based on NIST SP 800-162 (Reference 4) and the ABAC reference model used in the XACML standards (e.g., XACML 3.0) (Reference 1). Familiarity with those documents is assumed.

As used in this document, the term DPM encompasses the acts of dynamically creating, disseminating, and maintaining hierarchical rule sets to control digital resource management, utilization, and protection (Reference 3). These rule sets, or DPs, express ABAC policies that are used in ACMs to determine whether a subject is authorized to access an object.

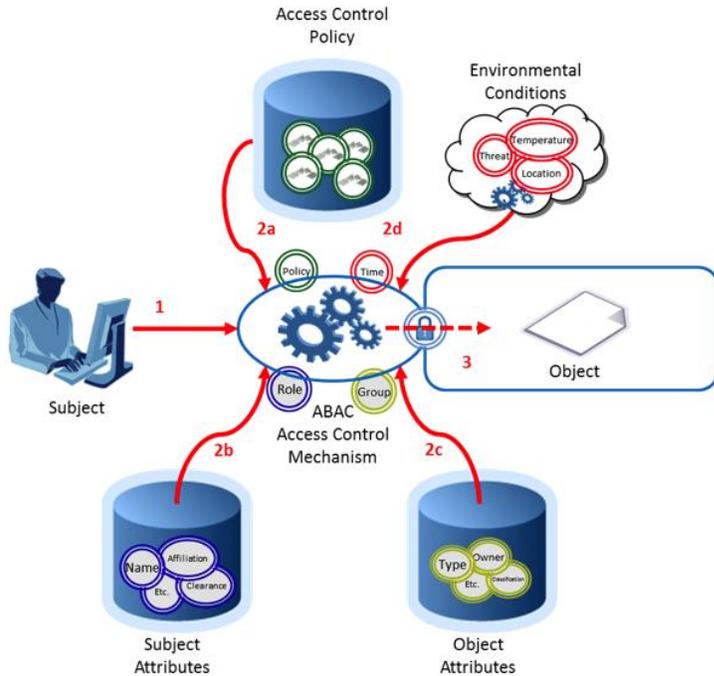
2.1 ABAC Concepts

Per NIST SP 800-162, ABAC is “an access control method where subject requests to perform operations on objects are granted or denied based on assigned attributes of the subject, assigned attributes of the object, environmental conditions, and a set of policies that are specified in terms of those attributes and conditions.” These policies can be represented as a set of relationships or rules; however, at a minimum, they must reflect the allowable set of operations the subject may perform upon the object if, and only if, the subject’s attributes and the environmental conditions meet those required for authorization given the object’s attributes.

Environmental conditions used in ABAC policies are represented by attributes that are not associated directly with subjects or objects. Rather, the environmental condition attributes (ECAs) are applicable across a defined portion of the systems implementing ABAC. Among other things, ECAs could include the current date and time, an indication of threat level [e.g., Information Operations Condition (INFOCON) 3], or a geographic location.

In the ABAC model, the ACM manages access decision, enforcement, and workflow. DPM functions ultimately provide DPs to ABAC ACMs for evaluation and enforcement. Figure 1, from NIST SP 800-162, shows the relationship of the fundamental elements required for ABAC authorization services. DPM is represented in the behind-the-scenes activities required to enable DP provisioning in Step 2a.

To better understand the makeup and use of a DP during an authorization transaction, it is important to understand the interactions that take place within the ACM. NIST SP 800-162 decomposes the ACM into a policy enforcement point (PEP), policy decision point (PDP), and **optional** context handler (CH). Figure 2, based on figures from NIST SP 800-62, shows these components of the ACM and their interactions with each other and with subjects, objects, policy retrieval points (PRPs), and policy information points (PIPs).



The ABAC in the figure controls the Subject's access to the Object by evaluating the Access Control Policy using the current values of the Subject Attributes, Object Attributes, and ECAs.

The numbered arrows represent the following actions:

1. Subject requests access to object
2. ACM assesses the following to determine authorization:
 - a) rules
 - b) subject attributes
 - c) object attributes
 - d) environmental conditions
3. Subject is given access to object if authorized and denied access if not authorized

Figure 1: Basic ABAC Model

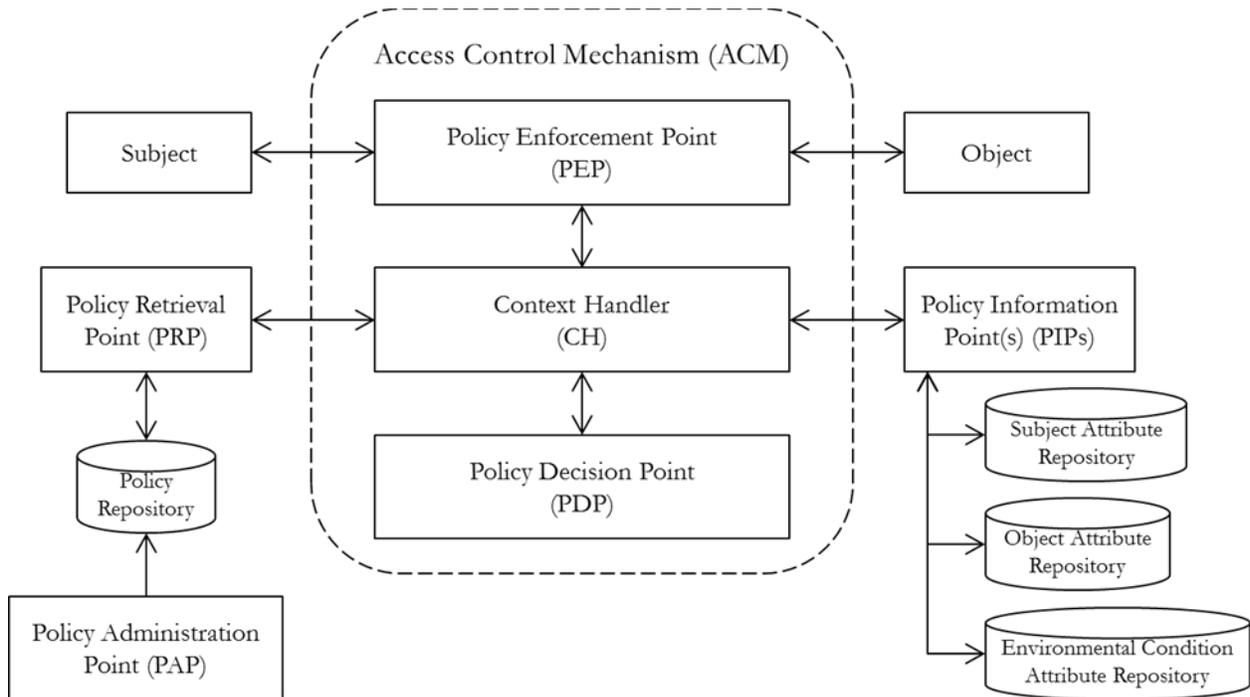


Figure 2: Decomposition of the ACM

The PEP serves as a gatekeeper, gathers subject and object identifying information, enforces the decision assertions of the PDP, and often performs authentication of the subject and object. The PDP evaluates policy and policy information (subject, object, and environmental condition

attributes), determines whether additional information is needed to satisfy a decision, and renders decisions. The CH coordinates the workflow for obtaining DP and policy information and presents that information to the PDP. The CH follows rules that designate the sequence, location, and handling requirements and other external interface and internal logical functions managed by the ACM. These CH rules may be embedded within DPs, hardcoded into the CH, or provisioned externally by a CH manager.

The CH is also responsible for handling obligations, which are additional actions required by the subject as a pre- or post-condition of granting authorization. Per XACML 3.0 (Reference 6), an obligation is “an operation specified in a rule, policy or policy set that should be performed by the PEP in conjunction with the enforcement of an authorization decision.” The following quote is also from XACML 3.0: “There are no standard definitions for these actions in version 3.0 of XACML. Therefore, bilateral agreement between a PAP and the PEP that will enforce its policies is required for correct interpretation. PEPs that conform to v3.0 of XACML are required to deny access unless they understand and can discharge all of the <Obligations> elements associated with the applicable policy.”

An obligation target (OT) embodies the PEP functionality needed to perform those required operations. The DP rules must express realizable obligations; that is, the rules must be created with knowledge of the OT functionality that is available in the PEPs. Some obligation functions may be present in all or most PEPs and some may be implemented in enterprise services that are called from the actual point of enforcement. The obligation functions of each PEP can be represented as ACM attributes that are known to the Policy Administrator (Admin) during the creation of DP.

Often, obligations are performed in conjunction with granting access to protect the object in transit using encryption or to alert the end user to the sensitive information using markings and warnings. Digital Rights Management protection might be added to restrict further dissemination of the object by the end user.

Another potential use of obligations in DP rules is to define the expiration conditions for the policy decision. This accounts for cases where some conditions that were true at the time of the policy decision may change later in a way that, if reevaluated, would change that decision. This can be important when policy decision assertions are cached for reuse when the same subject attempts access to other resources with the same access control attributes or when the policy decision results in persistent access to a resource, such as a user session, a virtual machine or a virtual network. For the persistent access case, expiration of a decision might not mean that the access is automatically terminated, but rather, that a reevaluation of policy is required to continue the access.

2.1.1 Identity/Subject Attribute Manager

The Identity/Subject Attribute Manager is the authority or set of authorities that issues subject attributes to subjects throughout the enterprise or organization. While predominately outside the scope of DPM, the Identity/Subject Attribute Manager must make subject attributes available for evaluation of DP as well as for preparation of DP. Information about the attributes (e.g., allowable

values, syntax) should be shared with Policy Stewards and Policy Admins to properly implement authorization conditions in DP for which the Identity/Subject Attribute Manager has a responsibility. The values of attributes used for access control must have high integrity. If high confidence in the attribute source or content is not assured, that may be noted in an ECA that is used in risk-adaptive policy decisions.

2.1.2 Object Owner

The Object Owner is the authority under which the object resides and who is responsible for protection of the object. Typically, the Object Owner is the head of the organization and is responsible for providing the access protections necessary to allow the object to be accessed only by authorized subjects. The Object Owner typically delegates management of objects and object attributes to one or more Object Stewards.

2.1.3 Object Steward

The Object Steward (sometimes referred to as a Data Steward) is the delegate manager of the objects and object attributes. The Object Steward is responsible for ensuring objects are marked appropriately or bound to tables with the correct object attributes, objects are sufficiently protected by ACMs, and appropriate policy is available to protect the objects in an ABAC model—a responsibility for which the Object Steward must coordinate with the Policy Steward.

Object attributes can be externalized from the objects and made available through an Object Attribute Retrieval Point (OARP) or somehow bound or tagged to the objects themselves. The Object Steward is responsible for ensuring that object attributes are correctly assigned to objects and that the CH rules reflect the appropriate means for obtaining the attributes associated with the object for which access is being requested.

While predominately outside the scope of DPM, the Object Steward, similar to the Identity/Subject Attribute Manager, must make object attributes available for evaluation of DP as well as for preparation of DP. Information about the attributes (e.g., allowable values, syntax) should be shared with Policy Stewards and Policy Admins to properly implement authorization conditions in DP for which the Identity/Subject Attribute Manager has a responsibility. The values of attributes used for access control must have high integrity. If high confidence in the attribute source or content is not assured, that may be noted in an ECA that is used in risk-adaptive policy decisions.

2.1.4 CH Owner

The CH Owner is the manager for the CH that establishes CH rules for use by the CH. The CH Owner is most often the ACM Owner or the Object Owner, but may be fulfilled by an enterprise entity that manages all CHs for an enterprise.

2.1.5 Object

The object is the information resource upon which the operation is to be performed. The object can be a service, application, file, file element (e.g., portion, paragraph, cell, or row), or any other information resource that requires protection from unauthorized operations.

2.1.6 Subject

The subject represents the entity requesting the authorization to perform an operation upon an object. Operations take the form of read, write, create, delete, or modify. The subject can be either a person or a non-person entity acting on behalf of a person.

2.1.7 Access Control Mechanism

The ACM is the entity that protects the object from unauthorized access by subjects. The ACM embodies the functionality of PEP and PDP. These functions may be flexibly implemented depending on the design required for the specific organization. For example, the CH functions can be executed by the PDP, or all three elements can be consolidated into a single ACM element. Additionally, these functions can be geographically or logically separated or distributed. For example, the PDP may be provided as an Enterprise Policy Decision Service (EPDS) where the CH functions are divided between the PEP and the EPDS.

2.1.7.1 *Policy Enforcement Point*

The PEP is the ACM component that enforces the decision and controls the subject's logical access to the object.

2.1.7.2 *Policy Decision Point*

The PDP is the ACM component that evaluates all of the inputs required for an access authorization decision and renders a decision. The decision can take the following forms:

- Allow Operation
- Deny Operation
- More Information Required
- Allow Operation with Obligations (obligations are activities required after the operation; e.g., protection of the data or expunging data after a period of time)

2.1.7.3 *Context Handler*

Per NIST SP 800-62 (Reference 4), the CH is the ACM component that manages the workflow and interfaces within and external to the ACM. The CH controls the following functions:

- Authentication with ABAC and DPM components
- Sequencing of policy and attribute retrieval
- Policy and attribute retrieval authoritative source location management

- Obligation processing
- Policy and attribute quality and assurance evaluation
- Attribute translation

The CH is managed by the CH Owner and provisioned with CH rules that define the specifics for each function. CH rules can be encapsulated within the object attributes, the applicable DP for a given object, or pre-provisioned to the CH as a set of DPs. Subsection 4.3.1 provides additional implementation considerations for the CH, CH rules, and obligations.

2.1.8 Obligation Target

The OT is the entity to which the CH must pass any authorization obligations for fulfillment. The OT could be an object, an external obligation management service, or another entity usually resident outside the ACM.

2.1.9 Policy Information Point

A PIP is one of many locations through which object, subject, and environmental condition attributes used in policy decisions are obtained. A PIP is the interface offered/exposed by attribute services for retrieval of attributes from attribute stores.

2.1.9.1 Object Attribute Retrieval Point

The OARP is a type of PIP through which object attributes, or resource metadata, are obtained. This may take the form of a service or a metadata file or may be pulled directly from the object itself.

Proper functioning of an ABAC authorization service requires a comprehensive and consistently implemented object attribute population or tagging capability. Without the proper object attributes available for policy evaluation, the ACM should default to deny access.

2.1.9.2 Subject Attribute Retrieval Point

The subject attribute retrieval point (SARP) is a type of PIP through which subject, or identity, attributes are obtained from Identity Management Systems.

2.1.9.3 Environmental Condition Attribute Retrieval Point

The environmental condition attribute retrieval point (ECARP) is a type of PIP through which the ECAs are obtained.

2.2 DPM Background

Although understanding of the ACM is crucial to understanding how ABAC pieces fit together, the majority of the DPM functions and capabilities reside elsewhere. Figure 3 expands the runtime activities related to access control policy to show a conceptual overview of the DPM functions that

are needed to provision DP for an Enterprise. The functions illustrated in the diagram can be implemented in many ways, with a mix of automated, semi-automated, and non-automated steps.

Borrowing from the DPM definition in Reference 1, DPM includes the ability to dynamically create, disseminate, and maintain hierarchical DP rule sets to control digital resource management, utilization, and protection. Using DP to enforce ABAC policies is the overall purpose of DPM, and that depends on the ability to assess DPs to ensure they collectively express the policy intent.

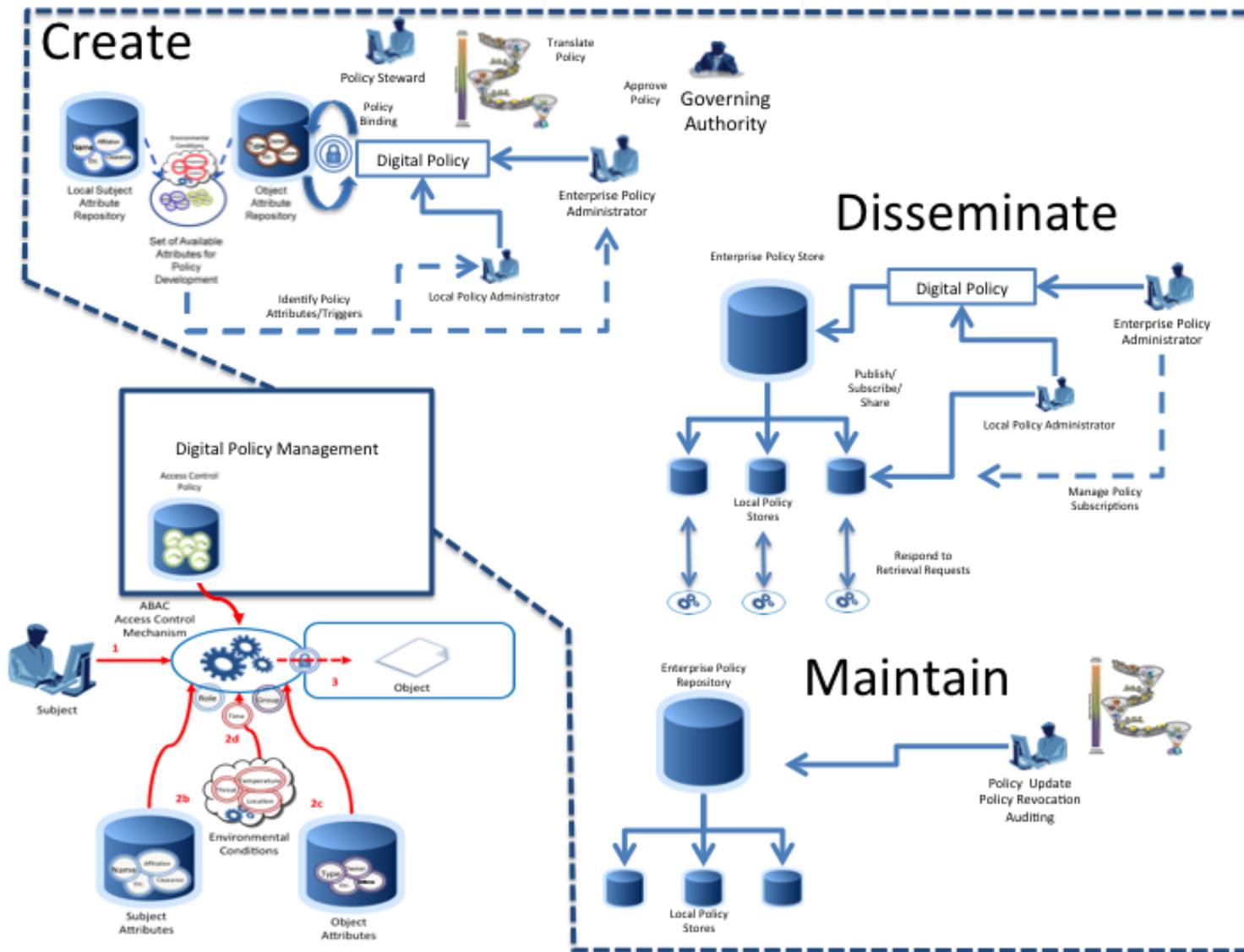


Figure 3: DPM Functional Overview

The Access Management Framework Tiger Team lists six Policy Administration Life Cycle processes (Reference 7) derived from the FICAM Roadmap and Implementation Guidance (Reference 2), as follows:

1. Definition
2. Analysis
3. Creation
4. Evaluation
5. Implementation and Enforcement
6. Review and Revision

Key to understanding DPM is an understanding of the states of DP as it transitions through the life cycle. These unique states of DP help identify the need for authorities, actors, and functions.

The following list of DP states introduces Human-Readable Structured Language Policy (HRSLP) as an **optional** interim step between Natural Language Policy (NLP) and DP that provides structured rule sets that are understandable by humans. HRSLP is not necessary for implementation of DPM but helps facilitate review and approval of policy when sharing DP or managing large volumes of DP in a large organization.

- **Approved HRSLP:** HRSLP that is approved by an appropriate authority based on evidence that, using available attributes, the HRSLP accurately represents the organization's policy intent. The policy intent is sometimes expressed as NLP. Prior to approval, HRSLP is in the Draft state.
- **Approved DP:** DP that is approved by an appropriate authority based on evidence that, using available attributes, the DP accurately represents the organization's policy intent. Proof of correspondence to Approved HRSLP may be used to support that approval decision. Prior to approval, DP is in the Draft state.
- **Verified DP:** DP that was Approved DP and has been deemed appropriate for dissemination and sharing after being assessed along with previously Verified DPs for potential conflicts and synergistic effects of policy combining by the PDPs.
- **Activated DP:** DP that was Verified DP and has been disseminated and/or shared for use in policy enforcement. Policy enforcement uses only Activated DP.
- **Retired DP:** DP that was Activated DP and has been removed from the set of DPs used in policy enforcement because it was revoked, replaced (updated), or expired.

3 DPM Capability Needs and Requirements

3.1 DPM Capability Needs

Table 2 describes the DPM capabilities needed to advance each DP through its states across the life cycle.

Table 2: DPM Capability Descriptions

Capability	Description	Life Cycle Processes	NLP and DP States
Policy Conversion	The ability to automatically or semi-automatically convert natural language laws, executive orders, regulations, directives, guidance, or rules into machine-readable DP.	Definition Analysis Creation	NLP Draft and Approved HRSLP Draft DP
DP Creation and Updating	The ability to create and update DPs. This can begin with Draft HRSLP and/or DP from Policy Conversion or with an understanding of the organization’s policy intent (with or without written NLP).	Definition Analysis Creation	NLP Draft and Approved HRSLP Draft DP
DP Content Approval	The ability to authoritatively determine that the DP accurately represents the policy intent of the organization and approve DP for use within the enterprise. This can include proof of correspondence with Approved HRSLP that was generated before or after DP generation.	Definition Analysis Creation	NLP Draft and Approved HRSLP Draft and Approved DP
DP Predictive Evaluation	The ability to evaluate a set of DPs for conflicts with other DPs and perform quality and consistency checks on the outcome of triggered DPs to validate that they will execute as intended.	Evaluation	Approved DP Verified DP
DP Activation and Retirement	The ability to manage the availability of DPs so that new and updated DPs that are activated are available to ACMs and expired and superseded DPs are retired and not available to ACMs.	Implementation and Enforcement	Activated DP Retired DP
DP Sharing	The ability to share DPs across policy domains. These domains can have hierarchical or peer relationships that reflect organizational structures. Authorities in the receiving domain may treat approved and activated policies as draft policies and perform their own content approval and predictive evaluation.	Definition Analysis Creation Implementation and Enforcement	NLP Approved HRSLP Approved DP Activated DP
DP Enforcement	The ability to respond to DP retrieval requests from ACMs. This is the DPM support provided to ACMs as they enforce the policies.	Implementation and Enforcement	Activated DP
DP Monitoring	The ability to audit and monitor active sets of DPs to evaluate authorities, currency, accuracy, and privileges imparted by the DPs and to identify the need for updating outdated or erroneous DP.	Review and Revision	Activated DP Retired DP

Table 2: DPM Capability Descriptions (Continued)

Capability	Description	Life Cycle Processes	NLP and DP States
DP Protection	The ability to protect the integrity, confidentiality, and availability of DPs. The integrity protection includes the ability to determine that an appropriate authority has transitioned the DP to its current state.	All	Approved DP Verified DP Retired DP

3.2 DPM Requirements

This section describes the DPM use cases and related ACM use cases that form the basis for DPM guidance. DPM functional requirements were derived from DPM use cases that provide the capabilities described in Section 3.1. System requirements (e.g., “The system shall...”) were derived from the use cases and are provided with unique numbering as an aid to requirements tracing. These functional requirements should always be applied in the context of the use cases and should not be used as standalone requirements.

This document makes reference to “use cases” as a means to describe the functional requirements of a system. For further information on use cases and use case diagrams, see the list of resources at www.uml.org (Reference 8).

The DPM use cases are as follows:

- Manage DP Content
- Approve DP Content
- Evaluate and Deconflict DPs
- Manage Activated DPs
- Enforce DPs
- Monitor DP Enforcement
- Import and Export Policies

Use case actors are the entities that interact with the DPM system during use case execution. The DPM use case actors are described next and shown in Figure 4, where the arrows in the figure indicate a generalization relationship (e.g., a Policy Steward is a type of DPM Stakeholder).

- **DPM Stakeholder (Human Actor):** All of the human actors for the DPM use cases are considered DPM stakeholders.
 - **Policy Authority:** The individual with the overall responsibility for an organization’s access control policies and for ensuring their compliance with legal constraints (e.g., laws, executive orders, regulations, directives, cross-organizational information sharing agreements).
 - **Enterprise Policy Authority:** The Policy Authority whose scope of responsibility extends to the entire Enterprise.

- **Local Policy Authority:** A Policy Authority whose scope of responsibility is limited to an organization within the Enterprise. Hierarchical organizations can have Local Policy Authorities at any layer of the organizational hierarchy. Local Policy Authorities may be accountable to an Enterprise Policy Authority for managing the dissemination and enforcement of Enterprise policies.
- **Policy Steward:** The individual who reports directly to a Policy Authority and is responsible for the management of ABAC DPs within his/her part of an organization so that those DPs are an accurate expression of the organization's current access control policy intent. That policy intent is often expressed in writing as NLP. As a minimum, the Policy Steward approves the content, effective date, expiration date, and supersession of each DP. For a small organization, the Policy Authority may choose to serve as the Policy Steward.
- **Policy Admin:** An individual who reports to a Policy Steward and is responsible for managing the content and/or dissemination of DPs.
 - **Policy Content Admin:** A Policy Admin responsible for managing the content of DPs.
 - **Policy Dissemination Admin:** A Policy Admin responsible for managing the dissemination of DPs. For a small organization, the Policy Content Admin and Policy Dissemination Admin responsibilities may be assigned to the same person.
- **External System (Non-Human Actor)**
 - **Other DPM Domain:** A DPM domain operating under a different Policy Authority. The Policy Authorities of two DPM domains may have peer or hierarchical organizational relationships.
 - **ACM:** The entity that protects the object from unauthorized access by subjects. The ACM embodies the functionality of PEP, PDP, and CH.
 - **PIP:** One of many locations through which object, subject, and environmental condition attributes used in policy decisions are obtained.
 - **SARP:** One of many locations through which subject attributes used in policy decisions are obtained.
 - **OARP:** One of many locations through which object attributes used in policy decisions are obtained.
 - **ECARP:** One of many locations through which ECAs used in policy decisions are obtained.

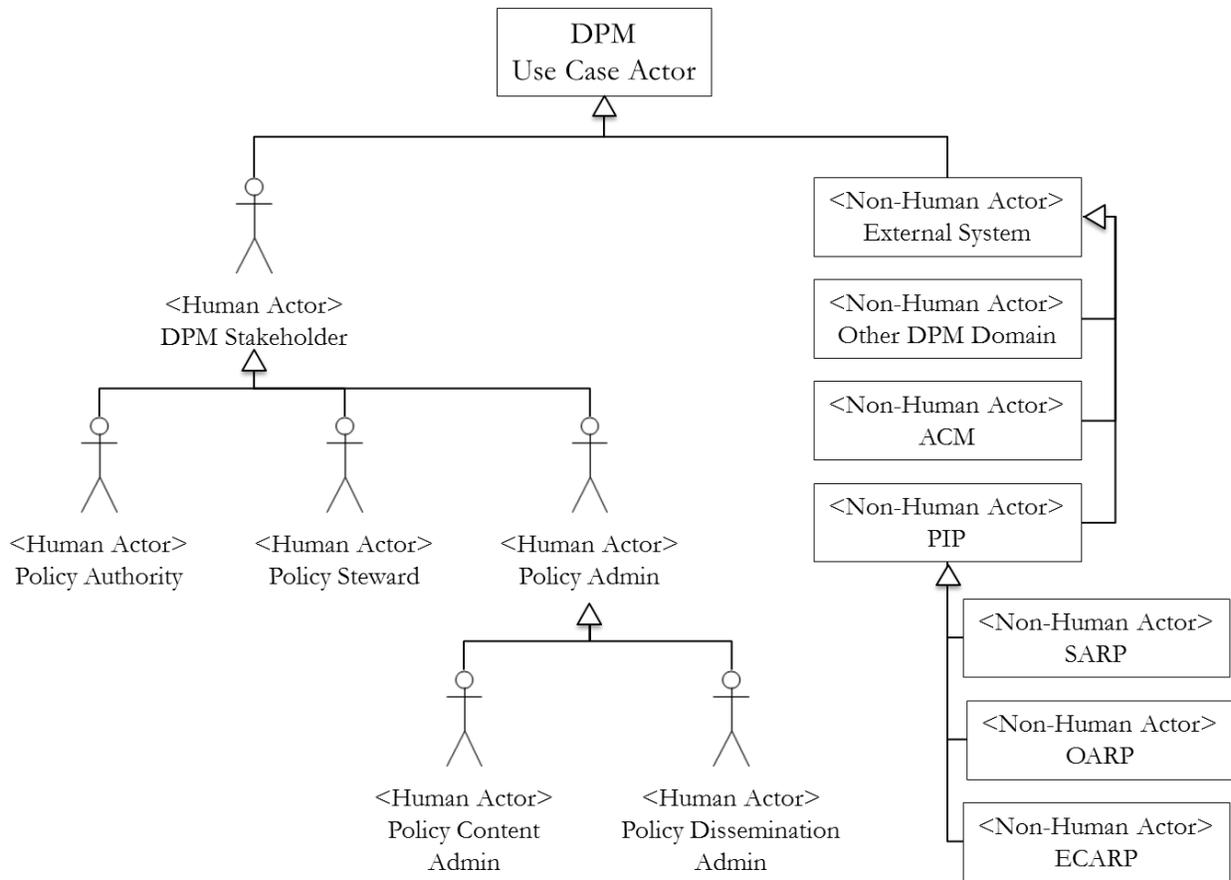


Figure 4: DPM Use Case Actors

Figure 5 presents a use case diagram showing all of the DPM for ABAC use cases and the external actors that interact with each use case. Most use cases are triggered by a human actor, but the Enforce DPs use case is triggered by a non-human actor (i.e., the ACM).

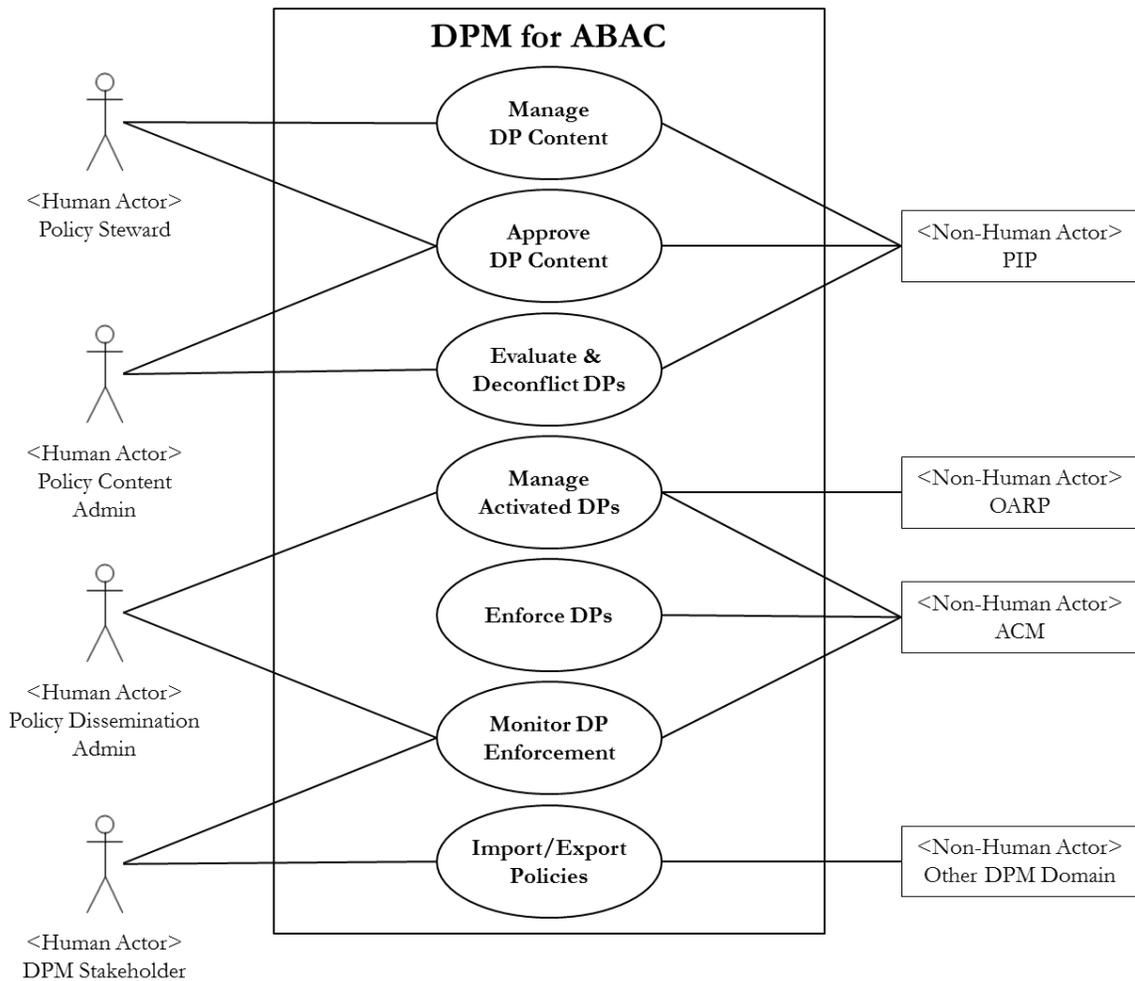


Figure 5: DPM for ABAC Use Case Diagram

A detailed description of each use case is provided in Table 4 to Table 10, using the format shown in Table 3.

Table 3: Use Case Description Format

Title	Use Case Title
Description	Overview description of the use case.
Actor(s)	One or more actors that interact with the DPM system during execution of the use case.
Trigger	The event that triggers the start of the use case.
Preconditions	A description of the conditions that must be true before the use case begins.
Postconditions	A description of the conditions that are changed by the execution of the use case.
Main Flow	A list of steps that are executed in the use case. The description of these steps is agnostic regarding the internal architecture of the DPM system.
Alternate Flows	A description of important exceptions to the main flow.
Requirements	A list of system requirements (e.g., “The system shall...”) derived from the use case. [A unique Requirement Number (Rqmt No.) is provided for each requirement as an aid to requirements tracing.]

Table 4: Manage DP Content Use Case Description

Title	Manage DP Content
Description	This use case describes how the actors listed in this table interact with the DPM system to create and/or update DP content.
Actor(s)	Policy Authority, Policy Steward, Policy Content Admin, PIPs
Trigger	A Policy Stakeholder provides instructions for creation or modification of DP content to correct a difference between the organization’s policy intent and the actual ABAC DPs in the Enterprise DPM. These instructions define the policy intent for controlling access using attributes of subjects, objects, and environmental conditions, including policy exception handling and policy obligations.
Preconditions	A Policy Stakeholder has identified a difference between the organization’s policy intent and the actual ABAC DPs being enforced. This can occur when (a) new NLP is provided by the Policy Authority, (b) new, unwritten policy intent is identified [e.g., creation of a new Community of Interest (COI) may imply the need for new ABAC rules for the subjects accessing objects in the COI], or (c) unexpected or unintended policy effects (including conflicts) are detected.
Postconditions	Draft DP content is proposed for use in the Enterprise ABAC enforcement (subject to approval, verification, and activation in other use cases). Draft DP includes assignment of (a) attributes that trigger application of the DP and, optionally, (b) authoritative sources of DP and attributes. Assignment of authoritative sources may be part of the ACM static configuration.
Main Flow (Manage DP Content when new NLP is provided by the Policy Authority)	<ol style="list-style-type: none"> 1. Policy Authority provides NLP to Policy Steward for translation to DP. This step, included to clarify responsibilities, is performed external to the DPM for ABAC system. 2. Policy Steward identifies attribute types needed for HRSLP and/or DP that would express the NLP. 3. Policy Steward verifies presence of attribute types in PIPs. If some attributes that are needed are not available, an ICAM use case would be initiated to make the needed subject, object, or environmental condition attributes available before proceeding. 4. Policy Steward translates NLP to HRSLP. Steps 4 through 6 may be omitted, at the Policy Authority’s discretion. <i>Note: Policy conversion can be a multi-step process and requires some form of semantic analysis or even interpretation of the written policy along with capturing the authority, applicability of the policy, rule sets, and time horizon of the policy.</i> 5. Policy Steward submits HRSLP and evidence that the HRSLP corresponds to the NLP to the Policy Authority for approval. 6. Policy Authority approves the HRSLP and returns Approved HRSLP to the Policy Steward. Disapproval may result in repeating steps 4 and 5. Policy Authority may choose to delegate this approval authority to the Policy Steward. 7. Policy Steward provides NLP and/or Approved HRSLP to Policy Content Admin for translation to DP. 8. Policy Content Admin translates NLP or Approved HRSLP to draft DP.
Alternate Flow (Manage DP Content when instructions are provided by Policy Steward or Policy Content Admin)	<ol style="list-style-type: none"> 1. Policy Steward or Policy Content Admin provides instructions for creation or modification of DP content. The instructions may include previously Approved DP or Activated DP that needs to be revised. The instructions must include the reason/intent for the new or revised policy. 2. Policy Content Admin identifies the attribute types needed for the new or revised DP. 3. Policy Content Admin verifies presence of attribute types in PIPs. If some attributes that are needed are not available, an ICAM use case would be initiated to make the needed subject, object, or environmental condition attributes available before proceeding. 4. Policy Content Admin creates or revises DP content.

Table 4: Manage DP Content Use Case Description (Continued)

<p>Requirements</p>	<p>Rqmt. No. 01. The system shall provide automated support for converting natural language laws, executive orders, regulations, directives, guidance, or rules to machine-readable policy.</p> <p>Rqmt. No. 02. The system shall provide authorized DPM Stakeholders the ability to create and update HRSLP in <TBD> format. Note: The <TBD> abbreviation is used to indicate that a standard format for HRSLP, once established, would be used in this requirement.</p> <p>Rqmt. No. 03. The system shall provide authorized DPM Stakeholders the ability to create and update DP in XACML 3.0 format. Note: Some organizations may have requirements for creating and updating additional XACML versions.</p> <p>Rqmt. No. 04. The system shall provide authorized DPM Stakeholders the ability to verify whether each attribute type and value used in HRSLP or DP is currently provisioned for use in policy decisions.</p> <p>Rqmt. No. 05. The system shall provide automated translation of HRSLP in <TBD> format to DP in XACML 3.0 format.</p> <p>Rqmt. No. 06. The system shall provide authorized DPM Stakeholders the ability to verify the correspondence between a HRSLP in <TBD> format and a DP in XACML 3.0 format.</p> <p>Rqmt. No. 07. The system shall provide authorized DPM Stakeholders the ability to assign an authoritative source for distribution of each DP.</p> <p>Rqmt. No. 08. The system shall provide authorized DPM Stakeholders the ability to map subject, object, and environment attributes that trigger the retrieval of each DP.</p>
----------------------------	--

Table 5: Approve DP Content Use Case Description

Title	Approve DP Content
Description	This use case describes how the actors listed in this table interact with the DPM system to evaluate and approve draft DP content that is compliant with policy intent for use in the Enterprise.
Actor(s)	Policy Steward, Policy Content Admin
Trigger	Policy Content Admin provides Draft DP (and optionally, Approved HRSLP) for approval.
Preconditions	Draft DP is proposed for use in the Enterprise.
Postconditions	Approved DP correctly expresses the organization’s policy intent.
Main Flow (Approved HRSLP is provided with the Draft DP)	<ol style="list-style-type: none"> 1. Policy Content Admin provides Approved HRSLP and Draft DP. 2. Policy Content Admin generates evidence that the Draft DP corresponds to the Approved HRSLP. This may include a formal proof of correspondence between the two forms of policy. 3. Policy Content Admin submits Draft DP and evidence that the Draft DP corresponds to the Approved HRSLP to the Policy Steward for approval. 4. Policy Steward approves and returns Approved DP to the Policy Content Admin. The Approved DP content is bound to the attributes defining its effective and expiration dates and its “Approved” status using the digital signature of the Policy Steward. Disapproval may result in returning to step 2 for more evidence or to the Manage DP Content use case for revision of the DP.
Alternate Flow (Approved HRSLP is not provided with the Draft DP)	<ol style="list-style-type: none"> 1. Policy Content Admin provides Draft DP. 2. Policy Content Admin generates evidence that the Draft DP corresponds to the policy intent. This may include translation of the Draft DP to Draft HRSLP and formal proof of correspondence between the two forms of policy. 3. Policy Content Admin submits evidence that the Draft DP corresponds to the policy intent to Policy Steward for approval. Approval indicates that the Draft DP correctly captures the policy intent that was provided in the alternate flow of the Manage DP Content use case and the evidence of correspondence is sufficient. 4. Policy Steward approves and returns Approved DP to Policy Content Admin. The Policy Steward may consult with the Policy Authority on this decision. Disapproval may result in returning to step 3 for more evidence or to the Manage DP Content use case for revision of the DP. When the evidence includes Draft HRSLP, this approval also results in Approved HRSLP being returned.
Requirements	<p>Rqmt. No. 09. The system shall provide automated translation of DP in XACML 3.0 format to HRSLP in <TBD> format.</p> <p>Rqmt. No. 10. The system shall provide authorized DPM Stakeholders the ability to verify the correspondence between a HRSLP in <TBD> format and a DP in XACML 3.0 format.</p> <p>Rqmt. No. 11. The system shall provide authorized DPM Stakeholders the ability to transfer a Draft DP to the Approved DP state.</p> <p>Rqmt. No. 12. The system shall distinguish between DPs in the following, mutually exclusive, states: Draft, Approved, Verified, Activated, and Retired.</p>

Table 6: Evaluate and Deconflict DPs Use Case Description

Title	Evaluate and Deconflict DPs
Description	This use case describes how the actors listed in this table interact with the DPM system to identify conflicts when an Approved DP is evaluated along with other applicable DPs and perform quality and consistency checks on the outcome of triggered DPs to validate that they will execute as intended.
Actor(s)	Policy Content Admin, PIPs
Trigger	Policy Content Admin provides Approved DP for analysis.
Preconditions	Approved DP is available for evaluation and deconfliction.
Postconditions	Approved DP is transitions to the Verified DP state.
Main Flow	<ol style="list-style-type: none"> 1. Policy Content Admin provides Approved DP for analysis. 2. Policy Content Admin identifies other DPs with overlapping policy attribute triggers. 3. Policy Content Admin analyzes the Approved DP for potential unresolved conflicts with the other DPs. 4. Policy Content Admin resolves any conflicts that are identified. Note: Resolution of conflicts may include rejection of the Approved DP, returning it to the Manage DP Content use case, or modification of the policy combining rules. 5. Policy Content Admin performs quality and consistency checks on the outcome of triggered DPs to validate that they will execute as intended. 6. Policy Content Admin resolves any unintended results. Resolution of unintended results may include rejection of the Approved DP, returning it to the Manage DP Content use case, or modification of the policy combining rules. 7. The Policy Content Admin transitions the Approved DP to the Verified DP state.
Requirements	<p>Rqmt. No. 13. The system shall provide authorized DPM Stakeholders the ability to evaluate a set of DPs for conflicts with other DPs.</p> <p>Rqmt. No. 14. The system shall provide authorized DPM Stakeholders the ability to perform quality and consistency checks on the outcome of triggered DPs to validate that they will execute as intended.</p> <p>Rqmt. No. 15. The system shall provide authorized DPM Stakeholders the ability to transfer an Approved DP to the Verified DP state.</p>

Table 7: Manage Activated DPs Use Case Description

Title	Manage Activated DPs
Description	This use case describes how the actors listed in this table interact with the DPM system to manage the dissemination of active DPs to ACMs for enforcement; ensure that DPs that are superseded, expired, or revoked are not available to ACMs; and provide CH Rules to ACMs.
Actor(s)	Policy Content Admin, Policy Dissemination Admin, ACM, OARP
Trigger	New Verified DP is available, Activated DP is identified for revocation and/or retirement, or an ACM subscription to Activated DPs is being updated.
Preconditions	Information is available to the Policy Dissemination Admin that allows a determination of the appropriate state and revocation status of the DPs and the subscription status of the ACMs.
Postconditions	Activated DPs are available for discovery and retrieval by ACMs. Retired, expired, and revoked DPs and those with effective dates in the future are not used by ACMs. Retired DPs are retained for use in audit analysis. ACM subscriptions are up to date.
Main Flow (New Verified DP)	<ol style="list-style-type: none"> 1. Policy Content Admin provides new Verified DP. 2. Policy Dissemination Admin reformats DP for use by ACMs. This may include transformation to stay within the constraints (e.g, XACML schema) of multiple ACM types. 3. Policy Dissemination Admin transitions the reformatted DP(s) to the Activated DP state and makes each Activated DP available for discovery and retrieval by ACMs. Only Activated DPs where the current date/time is between the effective and expiration date/time values are available for discovery and retrieval by ACMs.
Alternate Flow 1 (Supersede/Revoke/ Retire DP)	<ol style="list-style-type: none"> 1. Policy Content Admin or Policy Dissemination Admin identifies one or more DPs that should not be used for policy enforcement. Note: When new Verified DP supersedes existing Activated DP(s), this Alternate Flow is invoked along with the Main Flow. When Activated DPs are expired or revoked, this Alternate Flow is invoked without the Main Flow. 2. Policy Dissemination Admin ensures the DPs are not available to ACMs by adding them to a Digital Policy Revocation List (DPRL) and transitioning them to the Retired DP state. A DPRL is similar to a Certificate Revocation List in a public key infrastructure where the list is checked to determine whether the certificate (or in this case the DP) has been revoked prior to using it. Retired DPs may be physically removed from the stores that are accessible to ACMs, but they should be retained for use in audit analysis in the Monitor DP Enforcement use case.
Alternate Flow 2 (Manage DP Subscriptions)	<ol style="list-style-type: none"> 1. The Policy Dissemination Admin identifies an ACM that should have its Activated DP subscription updated. 2. The Policy Dissemination Admin updates the ACM subscription. 3. The Policy Dissemination Admin provides CH Rules to the ACM. A CH Owner, outside the set of DPM actors, may configure the ACM with the CH Rules.
Alternate Flow 3 (Bind DP to Objects)	<ol style="list-style-type: none"> 1. Policy Dissemination Admin binds applicable Activated DPs to objects and removes superseded, expired or revoked DPs. Note: This alternate flow is invoked along with the Main Flow, when there are ACMs that retrieve the DP with the other object attributes rather than through a separate DP discovery mechanism. 2. Policy Dissemination Admin updates object attributes with the applicable DP binding via an OARP. Note: This step assumes that the OARP can be used to post updates for object attributes.

Table 7: Manage Activated DPs Use Case Description (Continued)

Requirements	
	Rqmt. No. 16. The system shall provide authorized DPM Stakeholders the ability to transfer a Verified DP to the Activated DP state.
	Rqmt. No. 17. The system shall convert Activated DP, to specified formats as needed, for use by the ACMs.
	Rqmt. No. 18. The system shall provide authorized DPM Stakeholders the ability to publish Activated DPs to policy repositories.
	Rqmt. No. 19. The system shall provide authorized DPM Stakeholders the ability to disseminate updated versions of Activated DPs.
	Rqmt. No. 20. The system shall provide authorized DPM Stakeholders the ability to create, maintain, revise, search, and enforce a list of revoked DPs.
	Rqmt. No. 21. The system shall provide authorized DPM Stakeholders the ability to remove DPs that are revoked or expired from all policy repositories.
	Rqmt. No. 22. The system shall provide authorized DPM Stakeholders the ability to transfer an Activated DP to the Retired DP state.
	Rqmt. No. 23. The system shall provide authorized DPM Stakeholders the ability to archive Retired DP for use in monitoring and audit analysis.
	Rqmt. No. 24. The system shall provide authorized DPM Stakeholders the ability to enroll, subscribe, and unsubscribe to policy dissemination services provided by other policy repositories.
	Rqmt. No. 25. The system shall provide authorized DPM Stakeholders the ability to bind an object with the DPs that govern its protection, storage, modification, distribution, access, and deletion.
	Rqmt. No. 26. The system shall provide authorized DPM Stakeholders the ability to create and update CH workflow rules.
	Rqmt. No. 27. The system shall provide authorized DPM Stakeholders the ability to create and update CH assertion method rules.
	Rqmt. No. 28. The system shall provide authorized DPM Stakeholders the ability to create and update CH caching rules.
	Rqmt. No. 29. The system shall provide authorized DPM Stakeholders the ability to create and update CH DP retrieval location rules.
	Rqmt. No. 30. The system shall provide authorized DPM Stakeholders the ability to create and update CH DP authoritative source rules.
	Rqmt. No. 31. The system shall provide authorized DPM Stakeholders the ability to create and update CH PIP location rules.
	Rqmt. No. 32. The system shall provide authorized DPM Stakeholders the ability to create and update CH attribute authoritative sources rules.
	Rqmt. No. 33. The system shall provide authorized DPM Stakeholders the ability to create and update CH obligation methods rules.
	Rqmt. No. 34. The system shall provide authorized DPM Stakeholders the ability to create and update CH OT locations rules.

Table 7: Manage Activated DPs Use Case Description (Continued)

Requirements (cont'd)	Rqmt. No. 35. The system shall provide authorized DPM Stakeholders the ability to create and update CH workflow rules. Rqmt. No. 36. The system shall provide authorized DPM Stakeholders the ability to create and update CH exception handling methods rules. Rqmt. No. 37. The system shall provide authorized DPM Stakeholders the ability to create and update CH audit instructions rules.
------------------------------	--

Table 8: Enforce DPs Use Case Description

Title	Enforce DPs
Description	This use case describes how the DPM system provides Activated DPs to subscribed ACMs for use in ABAC policy enforcement.
Actor(s)	ACM
Trigger	ACM requests the DPs that are applicable to a subject request for access to an object under the current environmental conditions.
Preconditions	The ACM is subscribed to the published DPs and configured with CH Rules that govern the content and format of requests and the processing of responses.
Postconditions	The ACM has the Activated DPs that are needed to render an access control decision, enforce that decision, and satisfy policy obligations.
Main Flow	<ol style="list-style-type: none"> 1. ACM requests the DPs that are applicable to a subject request for access to an object under the current environmental conditions. 2. Applicable Activated DPs that are not expired, superseded, or revoked are returned to the ACM.
Requirements	<p>Rqmt. No. 38. The system shall return requested DPs to requesting ACMs.</p> <p>Rqmt. No. 39. The system shall ensure that expired or revoked DPs are not included in policy decisions.</p> <p>Rqmt. No. 40. The system shall return the most recent version of each applicable Activated DP that is effective and not expired or revoked in response to a DP request.</p> <p>Rqmt. No. 41. The system shall protect DPs and attributes used to render authorization decisions from unauthorized modification.</p> <p>Rqmt. No. 42. The system shall protect DPs and attributes used to render authorization decisions from unauthorized disclosure.</p> <p>Rqmt. No. 43. The system shall ensure that the DPs and attributes used to render authorization decisions were originated by authoritative sources.</p>

Table 9: Monitor DP Enforcement Use Case Description

Title	Monitor DP Enforcement
Description	This use case describes how the actors listed in this table interact with the DPM system to provide near-real-time situational awareness (SA) of policy compliance (i.e., the alignment of policy enforcement with policy intent) as well as after-the-fact analysis when problems are identified.
Actor(s)	Policy Dissemination Admin, DPM Stakeholder, ACM
Trigger	Policy Dissemination Admin identifies ACM and DPM mechanisms that should be monitored and audited.
Preconditions	Audit and sensor capabilities of ACMs are consistent with general security audit practices for access control. Audit and sensor capabilities of DPM mechanisms should allow monitoring of the dissemination of DP updates and revocations through the system.
Postconditions	DPM Stakeholders have SA views and audit reports that provide the current status of DP dissemination and enforcement.
Main Flow	<ol style="list-style-type: none"> 1. DPM Stakeholders requests ACM and DPM mechanisms audit and sensor data. Note: Requests for ACM data may be via security audit repositories. 2. DPM Stakeholders create SA views from current audit and sensor data in the context of the Activated DPs and the policy intent. 3. DPM Stakeholders analyze historical audit and sensor records in the context of Activated DPs and Retired DPs that were used in past enforcement to identify and diagnose cases where policy enforcement is not aligned with policy intent.
Requirements	<p>Rqmt. No. 44. The system shall provide authorized DPM Stakeholders the ability to monitor the dissemination of updated versions of Activated DPs.</p> <p>Rqmt. No. 45. The system shall provide authorized DPM Stakeholders the ability to receive audit records generated by ACMs.</p> <p>Rqmt. No. 46. The system shall provide authorized DPM Stakeholders the ability to perform audit analysis to verify policy compliance in DP enforcement.</p> <p>Rqmt. No. 47. The system shall provide authorized DPM Stakeholders the ability to get sensor data for near-real-time SA of policy compliance in DP enforcement.</p> <p>Rqmt. No. 48. The system shall provide authorized DPM Stakeholders the ability to synthesize SA views of the status of policy compliance in DP enforcement.</p>

Table 10: Import and Export Policies Use Case Description

Title	Import and Export Policies
Description	This use case describes how the actors listed in this table interact with the DPM system to send and receive policies (i.e., NLPs, Approved HRSLPs, Approved DPs, or Activated DPs) between DPM domains.
Actor(s)	DPM Stakeholder, Other DPM Domain
Trigger	A DPM Stakeholder identifies policies to be shared in a hierarchical relationship or under peer-to-peer information sharing agreements.
Preconditions	The policy aspects of the hierarchical relationships and peer-to-peer information sharing agreements are known to the DPM Stakeholders in both domains.
Postconditions	Applicable policies are shared across the DPM domains.
Main Flow (Export Policies)	<ol style="list-style-type: none"> 1. DPM Stakeholder identifies policies to be shared with the Other DPM Domain. 2. DPM Stakeholder sends identified policies to Other DPM Domain. Procedures established in the sending DPM domain determine which DPM Stakeholder sends which types of policy. For example, a Policy Steward or Policy Content Admin may be the only stakeholders allowed to send NLP and Approved HRSLP.
Alternate Flow (Import Policies)	<ol style="list-style-type: none"> 1. Policies are received from the Other DPM Domain. 2. DPM Stakeholders process the received policies. Policy processing includes execution of ICAM use cases involving the sending and receiving domains to ensure the Subject Attributes, Object Attributes, and ECAs in HRSLPs and DPs accurately reflect the policy intent (e.g., NLPs). Procedures established in the receiving DPM domain determine which DPM stakeholder processes each type of policy received and also determine whether the state of the policy in the sending domain is retained by the receiving domain. For example, Activated DP from another domain might be considered Approved DP in the receiving domain and require execution of the Evaluate and Deconflict DPs and Manage Activated DPs use cases before it is considered Activated DP in the receiving domain. The procedures of the receiving domain should be consistent with the hierarchical relationships or peer-to-peer information sharing agreements that govern the policy sharing.
Requirements	<p>Rqmt. No. 49. The system shall provide DPM Stakeholders the ability to share Approved DP and Approved HRSLP with other DPM Stakeholders to support cross-organizational information sharing.</p> <p>Rqmt. No. 50. The system shall provide DPM Stakeholders the ability to share Approved DP and Approved HRSLP with other DPM Stakeholders to support policy dissemination in hierarchical organizations.</p>

4 DPM Reference Architecture

4.1 DPM RA Overview

The proposed DPM RA detailed in this section helps to identify the fundamental components necessary to execute the management of DP within an enterprise. It introduces actors, functional entities and their capabilities, and a set of use cases to provide context for the architecture. Although the content in this section assumes a large enterprise—that of a D/A operating in the U.S. Federal Government—the entities and functions could be scaled down and simplified as long as the basic elements of DP creation, dissemination, and maintenance are performed.

The DPM RA assumes the implementation of a complementary set of capabilities needed to support ABAC within an enterprise, namely, an identity management capability that provides subject attributes and a set of object attributes assigned to the objects protected by the ACM. For the ABAC authorization use case, the DPM RA describes the actors, functional entities, capabilities, and use cases required to manage DP. This RA introduces some new concepts and terminology, but also attempts, where possible, to elaborate on already accepted concepts for the use of DP.

4.2 DPM Functional Components

This section details the key functional components required for supporting ABAC and DPM capabilities. These components were derived from the evaluation of DPM use cases and are deemed critical to the function of Enterprise ABAC and DPM. The functional components are described next, grouped by the major functional area they support.

- **DPM Stakeholder Interfaces**
 - The **Policy Administration Point (PAP)** provides the DPM Stakeholder interfaces used to trigger and execute use cases. Each PAP instance will have the user interfaces needed by its DPM Stakeholder user(s) to invoke and interact with the DP Content Management, DP Dissemination Management, and/or DP Enforcement Monitoring functional components. The PAP and other functional components used by DPM Stakeholders may be deployed on a single workstation or may be distributed in a client-server approach.
- **DP Content Management Components**
 - The **Policy Editor/Translator (PET)** provides translation and editing capabilities for HRSLP and DP.
 - The **Policy Analyzer/Simulator (PAS)** provides the ability to evaluate a set of DPs for conflicts with other DPs and perform quality and consistency checks on the outcome of triggered DPs to validate that they will execute as intended.
- **DP Dissemination Management Components**
 - The **Digital Policy Synchronization Manager (DPSM)** manages dissemination, update, and revocation of DPs.

- The **Local Digital Policy Repository (LDPR)** stores local and Enterprise-wide DPs for provisioning to assigned ACMs.
 - The **Enterprise Digital Policy Repository (EDPR)** stores Enterprise-wide DPs for provisioning to LDPRs and/or provisioning to ACMs.
 - The **Object-Policy Binding (OPB)** binds applicable DP to an object for dissemination as an object attribute via the OARP.
- **DP Enforcement Monitoring Components**
 - The **Policy Enforcement Situational Awareness (PESA)** gets sensor data from ACMs and from other DPM components for near-real-time SA of DP enforcement. The PESA synthesizes SA views of the status of DP enforcement.
 - The **Policy Enforcement Audit Analysis Tool (PEAAT)** receives audit records generated by ACMs and the DPM components and performs an audit analysis to verify the enforcement of DPs.
- **DP Enforcement Services**
 - The **Policy Retrieval Point (PRP)** is the entity through which the ACM obtains DPs from LDPRs and/or the EDPR. The PRP represents one or many locations through which DPs may be obtained. The PRP represents the local source of policies available to the ACM for decision and enforcement.
 - The **Digital Policy Revocation Service (DPRS)** is an **optional** mechanism through which outdated, erroneous, or otherwise deactivated policies are captured in a DPRL and made known to PRPs and ACMs by request. A DPRL is similar to a Certificate Revocation List in a public key infrastructure where DPM components evaluate the DPRL to determine whether the DP being used has been revoked prior to using it.

The DPM Functional Component grouping is illustrated in Figure 6. The policy store component is labeled as EDPR/LDPR because each DPM Stakeholder would be working with either of these policy repository types but probably not both.

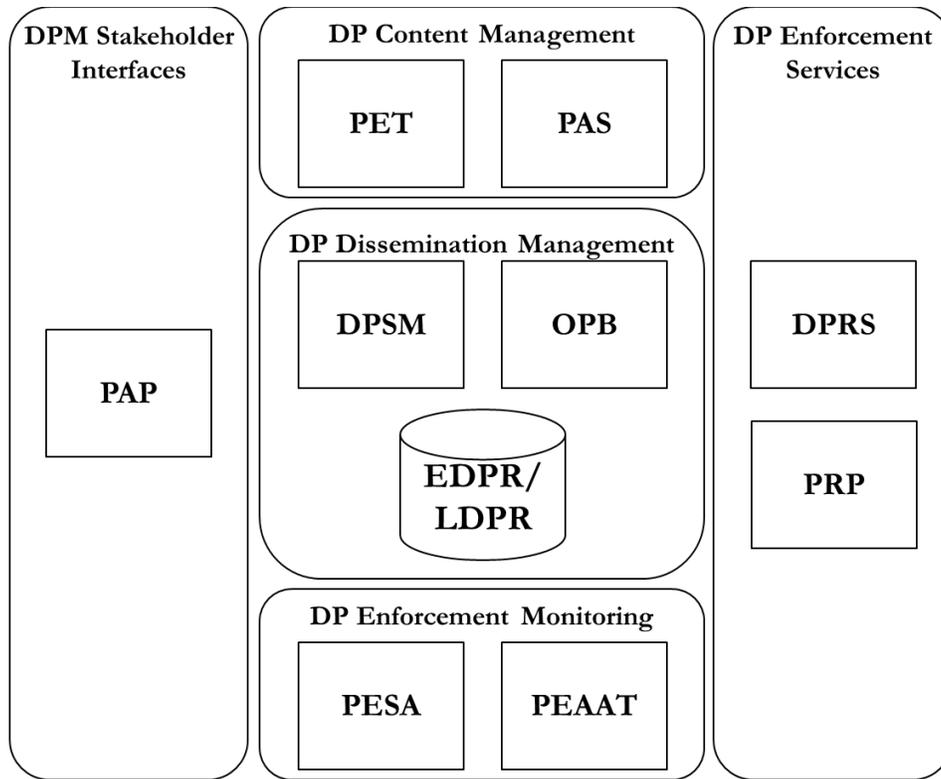


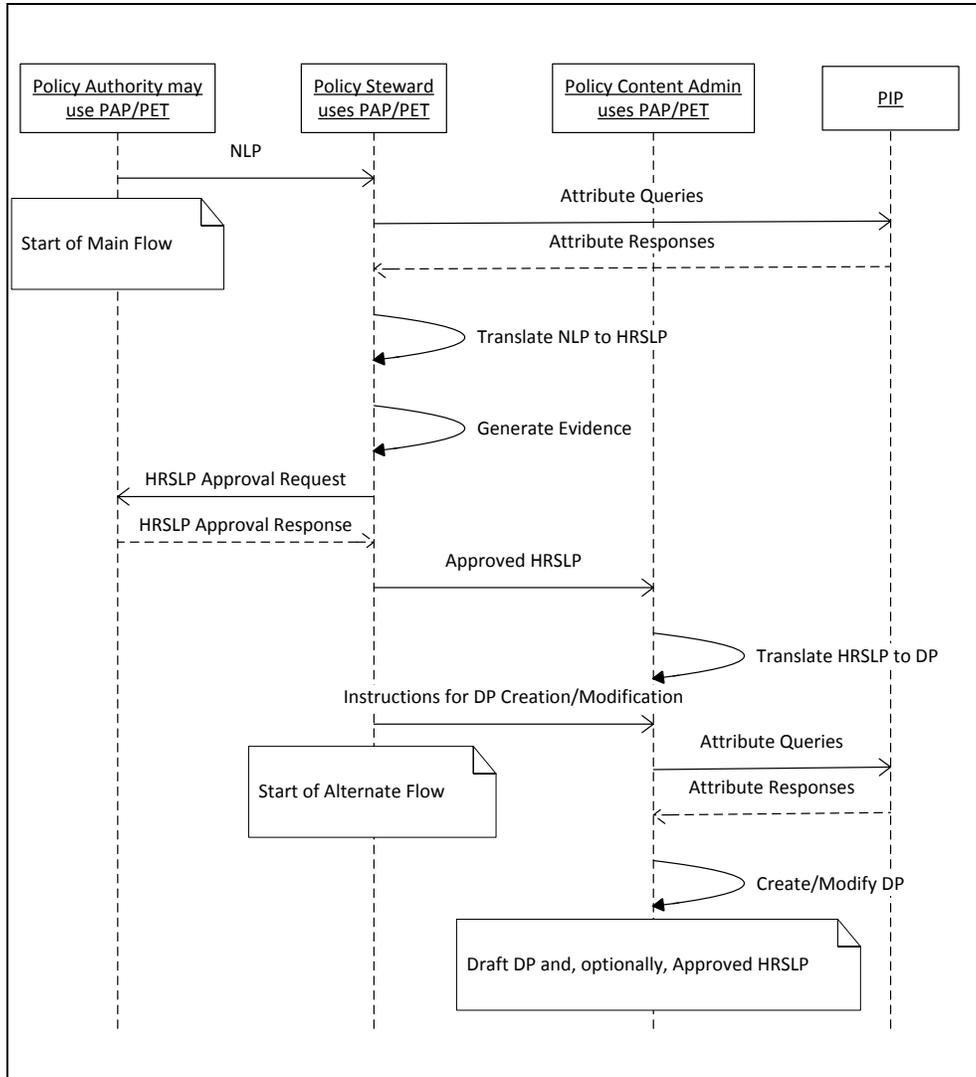
Figure 6: DPM RA Functional Components

4.3 Use Case Realization in the DPM RA

The following subsections describe the sequence of activities performed by DPM RA functional components in each use case.

4.3.1 Manage DP Content

Figure 7 shows the realization of the Manage DP Content use case in a sequence diagram. The Policy Authority, Policy Steward, and Policy Content Admin are the human actors involved in this use case. The DPM RA functional entities used by the human actors are the PAP and PET. The Policy Authority is either an Enterprise or local authority for the NLP. The PIP represents multiple external entities that are authoritative sources of attributes for subjects, objects, and environmental conditions.



The sequence diagram for each use case shows the ordering (from top to bottom) of the actor-initiated events and the data flows between entities. The ordering indicates a dependency between actions, unless the description says a step is optional or used "if needed." Arrows that begin and end on the same entity line represent steps that are completed by that entity without requiring interaction with others.

Figure 7: Sequence Diagram for Manage DP Content Use Case

4.3.2 Approve DP Content

Figure 8 shows the realization of the Approve DP Content use case in a sequence diagram. The Policy Content Admin and Policy Steward use the PAP and PET.

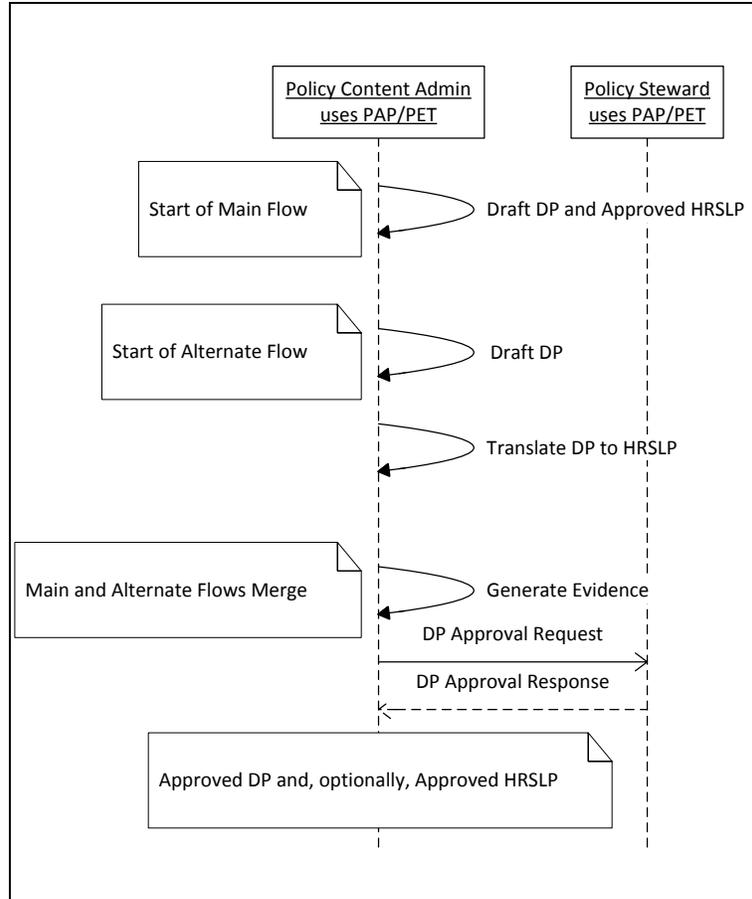


Figure 8: Sequence Diagram for Approve DP Content Use Case

4.3.3 Evaluate and Deconflict DPs

Figure 9 shows the use case steps in a sequence diagram. The Policy Content Admin uses the PAP user interface to move the Approved DP from the PET to the PAS and perform the analysis. The PRP is a non-human entity in the DPM RA.

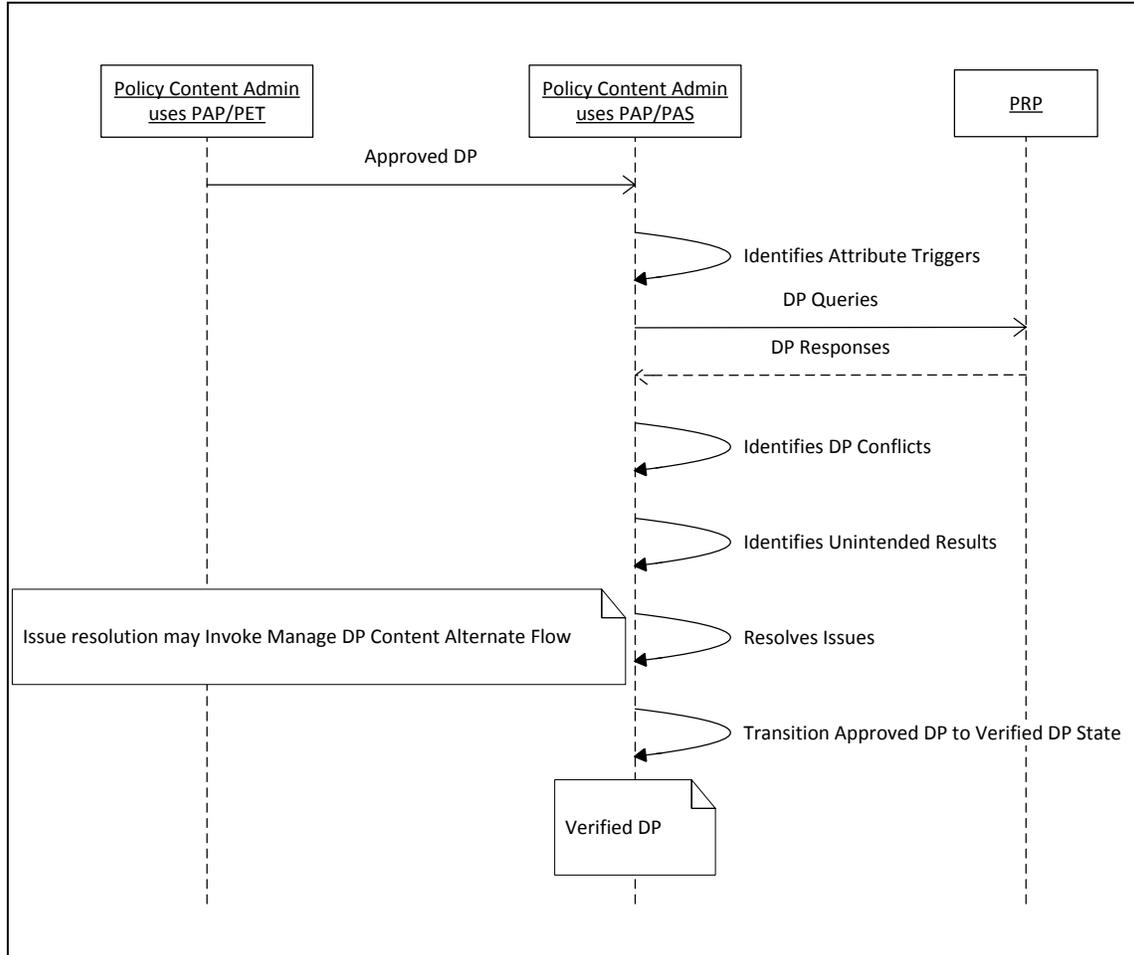


Figure 9: Sequence Diagram for Evaluate and Deconflict DPs Use Case

4.3.4 Manage Activated DPs

Figure 10 shows the use case steps in a sequence diagram. The Policy Dissemination Admin uses a PAP/DPSM to update ACM subscriptions by assigning them to one or more PRPs. The Policy Dissemination Admins uses the PAP/DPSM to activate policy and send it to EDPRs or LDPRs where they are made available to ACMs via a PRP. The Policy Dissemination Admin uses the PAP/DPRS to revoke DPs. The Policy Dissemination Admin uses the PAP/OPB to bind applicable policy to an object for dissemination through the OARP.

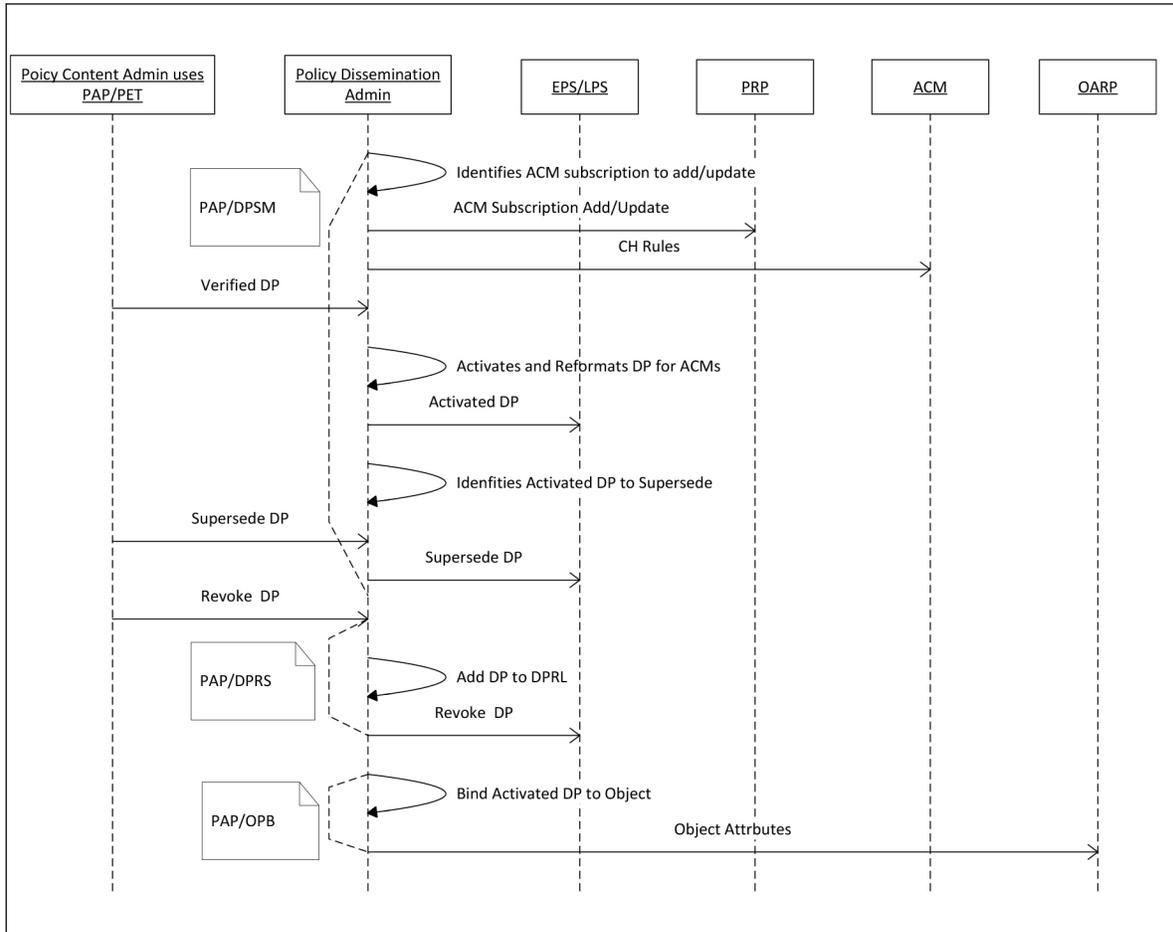


Figure 10: Sequence Diagram for Manage Activated DPs Use Case

4.3.5 Enforce DPs

Figure 11 shows the use case steps in a sequence diagram. Additional steps that are internal to the DPM system are added to show the role of each DPM entity. The ACM is an external non-human entity that obtains DPs from the policy repository via the PRP and DP revocation status of those policies from the DPRS. Although the PRP has performed the DP revocation status check, when DPs are cached by ACMs, the status can change between the time the PRP returns the DPs to the ACM and the time of enforcement, so another check may be needed.

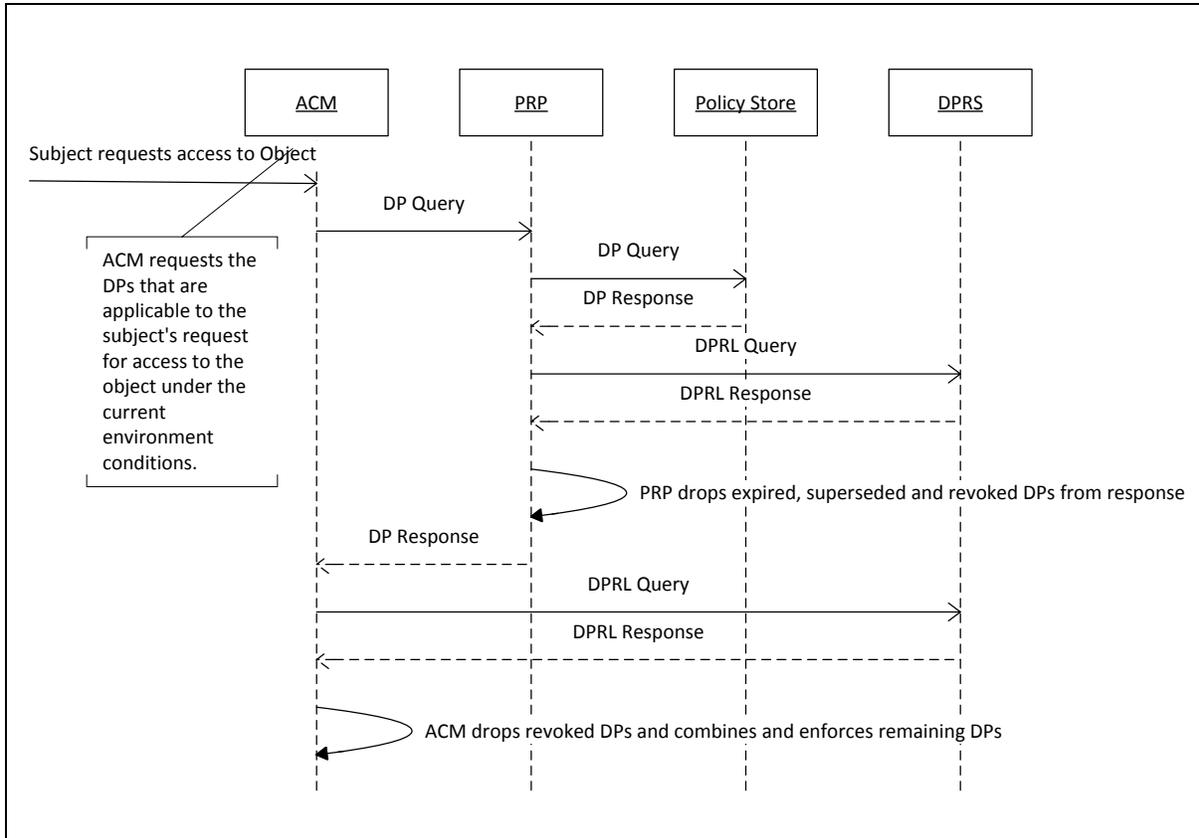


Figure 11: Sequence Diagram for Enforce DPs Use Case

4.3.6 Monitor DP Enforcement

Figure 12 shows the use case steps in a sequence diagram.

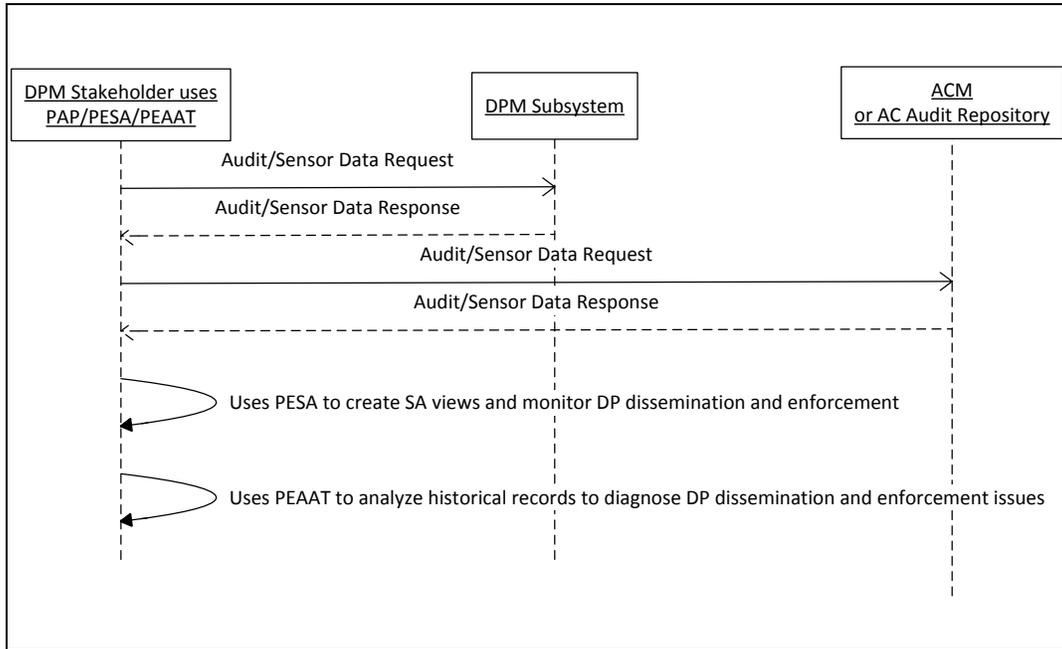


Figure 12: Sequence Diagram for Monitor DP Enforcement Use Case

4.3.7 Import and Export Policies

The implementation of the use case in the RA is a simple send/acknowledge message exchange between DPM Stakeholders in different organizations, as shown in Figure 13.

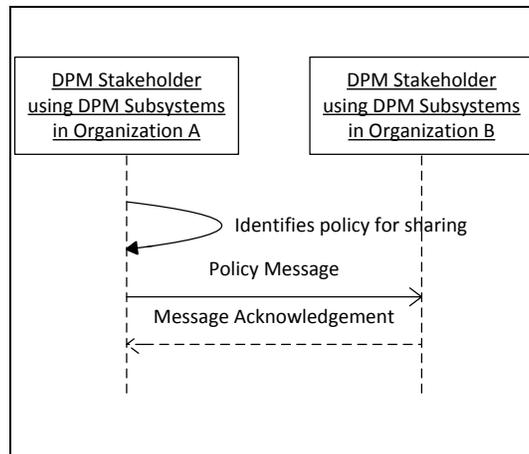


Figure 13: Sequence Diagram for Import and Export Policies Use Case

The DPM Stakeholder and policy types involved in the exchange will vary with the type of policy and established organizational procedures. Examples of DPM Stakeholders and policy types are as follows:

- Policy Authorities may send NLP external to the DPM ABAC system or delegate to Policy Stewards.
- Policy Stewards may send NLP and Approved HRSLP using PAP/PET.
- Policy Content Admins may send Approved DP using PAP/PET.
- Policy Dissemination Admins may send Activated DP using PAP/DPSM.

Procedures established in the receiving DPM domain determine whether the state of the policy in the sending domain is retained by the receiving domain. For example, Activated DP from another domain might be considered Approved DP in the receiving domain and require execution of the Evaluate and Deconflict DPs and Manage Activated DPs use cases before it is considered Activated DP in the receiving domain. The procedures of the receiving domain should be consistent with the hierarchical relationships or peer-to-peer information sharing agreements that govern the policy sharing.

4.3.8 DPM RA Data Model

The message types in the DPM RA use case realization are as follows:

- Policy Content (and acknowledgment response)
 - NLP
 - Approved HRSLP
 - DP
 - Approved DP
 - Verified DP
 - Activated DP
- Requests/Queries and Responses for
 - Policy Approval
 - HRSLP
 - DP
 - Attributes
 - Subject
 - Object
 - Environmental conditions
 - Audit/Sensor Data
- CH Rules

The XACML 3.0 specification (Reference 6) describes a policy language model for DP policy content that is sufficient for the DPM RA, with the addition of policy attributes to distinguish between Approved DP, Verified DP, Activated DP, and Retired DP. The XACML data model also describes attribute requests and responses. Standards establishing data models for the remaining message types should be developed as the DPM RA is being coordinated, revised and adopted.

5 DPM Implementation Considerations

This section discusses a diverse set of DPM implementation concerns that may or may not be adequately addressed in the RA.

As taken from Reference 3, DPM “includes identifying and adjudicating conflicts that may occur among existing and new rule sets due to the hierarchical and dynamic nature of policy. DP may define rules for authentication (trusted authorities, criteria for determining authenticity), authorization (access rules, authorized providers), quality of protection, quality of service, transport connectivity, bandwidth allocation and priority, audit, and computer network defense. DPM must protect digital policies, allowing only authorized subjects to create, modify, and delegate management of rules. It ensures proper implementation and enforcement of rules through interactions with policy engines and policy enforcement mechanisms and it provisions individual aspects of policy decisions to appropriate information assurance mechanisms.”

5.1 Protection of DP

The creation and modification of DP must be protected under the same or greater protections as the objects themselves. Only authorized Policy Stewards, Policy Authorities, and Policy Admins should have the ability to review or modify DP. DP repositories, PRPs, and PAPs should have appropriate access and authentication controls, and DPs themselves should be protected for confidentiality and integrity.

Protection of DP integrity can be implemented with time-stamped digital signatures prior to dissemination. If signature verification fails, due to error, failure, or unauthorized modification, the ACM should reject the DP and respond to the PRP so the Policy Dissemination Admin and/or Policy Content Admin can address the problem.

5.2 DP in an Information Sharing Environment

ABAC is primarily being implemented within the Federal Government to enable protected information sharing between D/As. DP will be used to protect Enterprise objects, and there are numerous considerations that need to be addressed when implementing DP in an information sharing environment.

Enterprise DP can be developed to address policy and object protection rules that apply to the entire enterprise—in this case, the entire Federal Government. The challenge is that, as the number of objects that need to be shared increases, it is unlikely that enterprise DP will be written to account for all objects, object attributes, and potential subjects and subject attributes that will be used by organizations—in this case, D/As. Although the Federal Government has made an effort to standardize a number of the subject attributes and object attributes that will be used by all D/As, there will be circumstances in which objects with nonstandard object attributes will be shared with organizations as well as subjects with nonstandard subject attributes.

When this occurs, it is important that the protections (codified in DP) placed on the object in its home organization be similarly placed on the object when it is shared or relocated to another organization. In this case, the DP must be transferred with the object, where binding DP to the object becomes useful; or the receiving organization's Object and Policy Stewards must develop new DP to reflect the new protections. In some cases, the object, subject, and environmental condition attributes must be modified or mapped to the corresponding attributes and attribute sources within the new organization.

5.3 Importance of the Context Handler

The CH is the “brain” behind several functions within the ACM. The CH manages the following:

- **Workflow:** What order to perform ACM functions (retrieve data, render decision, etc.) and where to go to retrieve and pass along information
- **Authentication:** Managing trust between all of the functional entities that interface with the ACM and validating and ensuring integrity of the assertions being handled or provided by the ACM or components within the ACM
- **Caching:** Storing and ensuring currency of information stored for evaluation by the ACM
- **Obligation Handling:** Executing obligations and forwarding them to the OT, identifying obligation enforcement violations, enforcing quality and confidence requirements of information being presented to the PDP, and evaluating and enforcing attribute assurance (currency, accuracy, authority, etc.)

As previously discussed, the functions within the ACM can be implemented in different ways. The ACM can be a single entity logically located adjacent to the object or the PEP, PDP, and CH functions can be segregated and logically distributed. When the PDP is provided as an enterprise service, the CH can be logically located with the PDP service, with the PEP protecting the object, or can be functionally split between the two. The functions within the CH can also be distributed and reside within any combination of the PEP and PDP.

Workflow within the ACM can be standardized or can be determined by the CH rules or DP. Standardized workflows work well in a small environment with static connections to the PDP, PEP, PIP, and PRP. Having the ability to externalize the management of the workflow provides flexibility to meet a wide array of use case requirements. For example, in the case of authorization of access to the object by the subject being time sensitive, it may be necessary to alter a standard workflow to prefetch attributes, DP, or even a decision prior to requesting access to the object. Another benefit of externalizing the management of the workflow is the flexibility to use different PIPs and PRPs depending on the object or object type being accessed.

Authentication with each of the entities with which the ACM interfaces provides integrity of the information being collected by, or passed from, the ACM. Concerning ACM functionality, when PIPs and PRPs are distributed in a large enterprise, this function becomes extremely important.

There are many authentication methods that can be used; however, most require some form of external key or token management function to ensure objective verification of credentials.

Enforcing quality and confidence of the information collected by the ACM requires some kind of measurement system to qualitatively provide a level of confidence or quality to the data being evaluated. If data are old, provided by less authoritative sources, or originally collected using less accurate methods, the quality or confidence score will be lowered. When evaluating that information for authorization decisions, it may not meet a policy threshold for quality and confidence of the information. This concept may be implemented by building policy to evaluate information quality and confidence attributes—essentially, attributes about the attributes used in the decision.

5.4 Human-Readable Structured Language Policy

HRSLP is an **optional** tool that may be used to assist in the conversion of NLP to DP. In its machine-readable format, human decision makers may not easily understand DP. The development of DP directly from NLP can be performed by a developer, assisted with the use of a semantic tool that helps convert NLP statements to DP, or through an intermediary step that structures rules the way they would be implemented in DP but in a more easily understood format for human decision makers to review and approve—or HRSLP. HRSLP provides a way for senior leadership to understand the rule sets being applied to an enterprise or organization and provide a way to maintain traceability from the NLP to the DP.

Table 11 describes one recommended approach for structuring the HRSLP policy and context information that is necessary to create DP from NLP.

Table 11: HRSLP Policy and Context Information

Element	Description
Policy Identification	Unique identification for the policy.
Rule Identification and Version	Unique identification for the subordinate rule set reflected in this document.
NLP Reference	Source NLP and sections this policy reflects.
NLP Authority	Authority under which the NLP was written and for which this HRSLP and subsequent DP is written.
NLP Context	Context for which this policy is applicable. This should reflect the scope and applicability of the policy as well as the situations for which the policy is meant.
NLP Intent	Plain language intent of the NLP. This should be a high-level statement for the intent of the source NLP.
Rule Intent	Plain language intent of the rule or NLP quote. This should be easily understood by anyone and reflect both the intent and the parameters of the rule.
Valid For	Date and time limitations for rule validity. Every rule should have a default end date or review date.
Authored By and Date	Name of HRSLP author (usually the Policy Steward), organization, and date when written.
Organization	Organization for which the rule will be implemented.

Table 12 provides a recommended approach to structuring HRSLP rule sets.

Table 12: Recommended Structure for HRSLP Rules

Element	Description	Example	
Subject with Subject Attributes...			
Operator	AND/OR	AND	
Subject Attribute	Attribute Name	Role	Privacy Training Status
Subject Attribute Value	Attribute Value	Organization A Manager	Current
Subject Attribute Authority	Attribute Authority	Identity Manager	Training Manager
Subject Attribute Location	Logical location where Subject attribute may be retrieved	https://www...	https://www...
May Perform Operations...			
Operator	AND/OR	N/A	
Operation	Create, Read, Write, Modify, Delete, etc.	Modify	
Upon Objects with Object Attributes...			
Operator	AND/OR	AND	
Object Attribute	Attribute Name	Object Type	Object Organization
Object Attribute Value	Attribute Value	Staff Record	Organization A
Under Environmental Conditions...			
Operator	AND/OR	N/A	
ECA	Attribute Name	Time	
ECA Value	Attribute Value	Organization A Working Hours	
ECA Authority	Attribute Authority	Organization A Time Authority	
ECA Location	Logical location where the ECA may be retrieved	https://www...	
With the Following Obligations...			
Obligation	External requirement imposed when authorization granted	Modifications must be audited by Human Resources (HR) representatives	
OT	External entity upon which the obligation is imposed	HR workflow	
Enforcement Mechanism	Description of the policy or technical enforcement mechanism to be used to enforce the obligation	Modifications not reviewed within 3 days are flagged	
Enforcement Responsibility	Organization entity responsible for enforcing the obligation	Organization A HR	

Table 12: Recommended Structure for HRSLP Rules (Continued)

Element	Description	Example
Under Environmental Conditions...		
Exception Condition	Anticipated circumstances where rule or obligations may be modified in real time; this optimally should be reflected in policy, but there are circumstances where this mechanism may be necessary	Access is denied because the subject's role is not considered as mission "need-to-know" for the object.
Exception Authority	Authority that can grant exception	Mission Manager may establish need-to-know without updating subject's attributes.
Exception Revisions	New rule or obligation that is in effect if the exception circumstances are experienced	Only applies if all other attributes are satisfactory.

5.5 DP Feedback and Override

The response provided by an ACM to a requesting person or non-person entity when access is denied may include information on the conditions that caused the deny decision. The requesting entity may use the response information to pursue changes to those conditions (i.e., identity, object, and environment attributes) that would change the decision outcome. The requesting entity may be assisted in this process by way of access to metadata that is less sensitive than the requested resource it describes.

The ACM feedback functionality and interface to the requesting entity are outside the scope of the DPM RA. Creation of less sensitive metadata is also outside the scope. A predefined workflow may be available to the requesting entity for changing the conditions, and this may include a second entity that is authorized to override the original access decision. This override authority can be expressed several different ways in the DP rules. Two of those approaches are described next, along with the DP implications:

- **Identity attribute approach:** The override authority can endorse the specific request, and the binding of the authority's identity attributes in the endorsement to the request will result in a decision to grant access. The two-entity request approach requires that DP rules account for such requests and that ACMs can process those requests.
- **ECA approach:** The override authority can set an ECA with scope that is limited. DP rules would evaluate to a grant decision for certain combinations of attributes that include the override attribute. The authority would have permission to set the attribute for a given scope. The scope could be limited to the user's specific request, the user's session, a specific time frame, or a set of users in specific roles.

5.6 Caching Assertions

If requests for attributes, DPs, DPRLs, and decisions are performed for each access attempt, the networks will be filled with those requests and responses and the access decisions may be delayed for a time that would be noticeable to the users. A common pattern for reducing the number of requests and responses and reducing the latency in processing is to cache the response assertions locally for use in another decision that uses the same DP or the same attributes. If the DP and attributes are the same, the policy decision assertion could be reused. However, this approach for making the decision process more efficient will introduce errors when DPs, DPRLs, and attributes are updated between the time the assertion is received and when it is used in enforcement.

To manage the errors and the risks they cause, a caching policy is needed. This caching policy could be part of the CH rules, part of the DP, or part of the assertion itself. It would define the validity time period for cached assertions from DP, DPRL, PIP, and PDP responses.

The selection of the validity time period is a risk management decision based on the harm that could come from errors in policy decisions. For example, an organization may choose to allow DP, PIP, and PDP responses to be cached for a 24-hour period, but require DPRL requests for each access attempt. The organization should monitor the performance effects and the errors caused by assertion caching and should update the validity time periods to balance performance with risk.

6 DPM RA Technology and Standards Overlay

This section discusses the suitability of the current and planned technologies and standards for implementation of the DPM reference architecture. It also includes recommendations for implementing Enterprise-wide, cross-organizational DPM.

6.1 Current and Planned Technologies and Standards

6.1.1 Technologies

A market survey (Reference 9) of DPM-capable products indicates that there are viable products that perform many of the Enterprise DPM functions. Most of the products surveyed are part of a suite that includes policy decision and enforcement, and most support XACML as the policy language. Use of the XACML standard suggests that a heterogeneous mix of these products could be used to implement PDPs and PEPs, while choosing a smaller subset for the DPM functionality. Few of these products allow the separation of PDP and PEP, and most employ some form of proprietary interface between PDP and PEP.

One major gap in DPM functionality for these products is the automated support for translation of NLPs and business rules into DP. The absence of this function is an indicator of the difficulty in performing the automated translation. Capturing the intent of NLPs and business rules requires knowledge of the mission or business domain terminology; therefore, a trial-and-error approach with correction based on user feedback is required. Also, the translation function must be able to take into account the target system's specific implementation of ABAC, including the following:

- Attributes used to represent the policy-relevant characteristics of resources, subjects, and environment
- PEP capabilities to act as OTs (i.e., to fulfill obligations such as generation of provenance records or displaying warning banners to users) or other logic required by the ACM
- Desired workflow order and interface requirements for the CH contained within the ACM

Only a few products support auditing and monitoring of the operational effects of either changing DPs or delaying the dissemination of those changes. It is not clear whether those products could be used to monitor the effects for policies generated and disseminated by products from other vendors.

In general, no CH or DPSM products meet the various functional requirements illustrated in Figure 2. Additionally, few of the products are designed to manage DP distribution, update, or revocation across a large enterprise, and most are designed to operate within a well-defined system or network boundary.

During the market research, two vendors announced that their products were being discontinued. Also, the literature on the reviewed products indicated the vendors were adapting the products as they discovered new requirements while working with their customers. This rapid change in

available technologies would make any recommendation of specific technologies become outdated during the vetting for inclusion in the FICAM Roadmap and Implementation Guidance.

6.1.2 Technology Development Efforts

The development efforts identified in Reference 9 focused on *policy authoring*, including translation from NLPs to DPs, and *policy auditing*. These two areas, along with OPB and assigning policy triggers, have the least amount of coverage by the commercial products reviewed. Less obvious in the review of products is the lack of tools for managing the entire policy rule set life cycle in an enterprise setting that includes a heterogeneous mix of ACMs.

6.1.3 Standards

The standards reviewed in Reference 9 were either architecture standards that provide broad guidance for implementing DPM capabilities or interface standards that define formats and/or protocols for posting and retrieving DP, attributes, and policy decisions.

Some of the interface standards (e.g., XACML and Security Assertion Markup Language) are used by many of the products reviewed. There are no standards for HRSLP, but two vendor products offer the policy author a graphical interface that creates a structured (code-like) expression that is compiled into XACML. The lack of an HRSLP standard is an impediment to a standardized Enterprise approach for policy authoring, validation, and approval. In the absence of such a standard, one or more proprietary approaches are likely to emerge.

The U.S. Department of Defense documents discussed in Reference 9 are architecture standards that offer only high-level direction to include policy management in the Enterprise. The NIST documents provide more detailed guidance on ABAC and establish important concepts of DPM.

6.2 Implementation Recommendations

The following implementation recommendations are provided for consideration by the FICAM community:

Recommendation 1: Review, revise, and approve the DPM RA.

This should include:

- Coordinating this document with D/As and interdepartmental working groups.
- Updating FICAM Roadmap and Implementation Guidance documents to reflect the approved DPM RA.

Recommendation 2: Establish best practices for approval of HRSLP and DP.

This should include:

- Establishing a standard format for HRSLP.
- Using a risk-driven approach for defining the evidence required for approval.

Recommendation 3: Use the approved RA in acquisition strategy.

This should include:

- Offering this document for consideration in establishing a NIST SP that augments NIST SP 800-162 with additional DPM detail.
- Using the functional requirements to drive commercial and Government-funded development of Enterprise-wide DPM capabilities.
- Deriving criteria from the requirements for use in trade studies comparing commercial technologies.
- Identifying critical functionality that should be developed or accelerated with Government funding.

Appendix A

References

1. “Framework” definition, retrieved from whatis.com, 3 December 2014
[<http://whatistechtarget.com/search/query?q=framework>]
2. *Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance*, Version 2.0, 2 December 2011
[http://www.idmanagement.gov/sites/default/files/documents/FICAM_Roadmap_and_Implementation_Guidance_v2%2020111202_0.pdf]
3. Committee for National Security Systems, *Identity, Credential, and Access Management Capabilities (ICAM) Lexicon*, Version 1.0, 30 May 2013
[<http://www.idmanagement.gov/sites/default/files/documents/NSS%20ICAM%20Lexicon%20v1%2030MAY13.pdf>]
4. NIST SP 800-162, *Guide to Attribute-Based Access Control Definition and Considerations*, January 2014 [<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-162.pdf>]
5. CNSSD 507, *National Directive for Identity, Credential, and Access Management Capabilities (ICAM) on the United States Federal Secret Fabric*, January 2014
[<https://www.idmanagement.gov/sites/default/files/documents/National%20Policy%20for%20ICAM%20on%20the%20Secret%20Fabric%20v1%200.docx>]
6. Organization for the Advancement of Structured Information Standards (OASIS) Standard, *eXtensible Access Control Markup Language (XACML)*, Version 3.0. 22 January 2013
[<http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html>]
7. *Access Management Policy Framework*, Draft, July 2014
8. *Unified Modeling Language (UML) Resource Page*, retrieved from www.uml.org, 3 December 2014 [<http://www.uml.org/>]
9. *Digital Policy Management Market Survey*, 7 August 2014
10. *A Brief Introduction to XACML*, March 2003 [https://www.oasis-open.org/committees/download.php/2713/Brief_Introduction_to_XACML.html]
11. Office of Management and Budget Memorandum 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, 22 May 2007
[<http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf>]

Appendix B Acronyms

Terms with an asterisk are defined in the Glossary (Appendix C).

ABAC	Attribute-Based Access Control*
ACM	Access Control Mechanism*
Admin	Administrator
CH	Context Handler*
CNSSD	Committee for National Security Systems Directive
COI	Community of Interest
D/A	Department and Agency
DP	Digital Policy*
DPM	Digital Policy Management*
DPRL	Digital Policy Revocation List*
DPRS	Digital Policy Revocation Service*
DPSM	Digital Policy Synchronization Manager*
ECA	Environmental Condition Attribute
ECARP	Environmental Condition Attribute Retrieval Point*
EDPR	Enterprise Digital Policy Repository
EPDS	Enterprise Policy Decision Service
FICAM	Federal Identity, Credential, and Access Management
HR	Human Resources
HRSLP	Human-Readable Structured Language Policy*
ICAM	Identity, Credential, and Access Management
INFOCON	Information Operations Condition
LDPR	Local Digital Policy Repository
NIST	National Institute of Standards and Technology
NLP	Natural Language Policy
OARP	Object Attribute Retrieval Point*
OASIS	Organization for the Advancement of Structured Information Standards
OPB	Object-Policy Binding
OT	Obligation Target*

PAP	Policy Administration Point*
PAS	Policy Analyzer/Simulator
PDP	Policy Decision Point*
PEAAT	Policy Enforcement Audit Analysis Tool
PEP	Policy Enforcement Point*
PESA	Policy Enforcement Situational Awareness
PET	Policy Editor/Translator
PIP	Policy Information Point*
PRP	Policy Retrieval Point*
RA	Reference Architecture
SA	Situational Awareness
SARP	Subject Attribute Retrieval Point*
SP	Special Publication
XACML	Extensible Access Control Markup Language
XML	eXtensible Markup Language

Appendix C Glossary

If no reference is cited, the term is a concept that is introduced and explained within the body of this document.

Term	Definition	Reference
Access Control	The process of granting or denying specific requests: (1) for obtaining and using information and related information processing services and (2) to enter specific physical facilities (e.g., Federal buildings, military establishments, and border crossing entrances).	3
Access Control Mechanism	The entity that protects the information and related information processing services from unauthorized access.	
Activated DP	DP that was Verified DP and has been disseminated and/or shared for use in policy enforcement.	
Approved DP	DP that is approved by an appropriate Policy Steward, based on evidence that, using available attributes, it accurately represents Approved HRSLP.	
Approved Human-Readable Structured Language Policy	HRSLP that is approved by an appropriate Policy Authority or, when delegated, a Policy Steward, based on evidence that, using available attributes, it accurately represents the organization's policy intent. <i>Note: That policy intent is sometimes expressed as NLP.</i>	
Attribute	A claim of a named quality or characteristic inherent in or ascribed to someone or something.	3
Attribute Authority	An entity recognized as having the authority to verify the association of attributes to someone or something.	3
Attribute-Based Access Control	Access control based on attributes associated with and about subjects, objects, targets, initiators, resource, or the environment. <i>Note: An access control rule set defines the combination of attributes under which an access may take place.</i>	3
Audit	Independent review and examination of records and activities to assess the adequacy of system controls and ensure compliance with established policies and operational procedures.	3
Context Handler	The system entity that converts decision requests in the native request format to the XACML canonical form, coordinates with PIPs to add attribute values to the request context, and converts authorization decisions in the XACML canonical form to the native response format. <i>Note: The CH is part of the ACM.</i>	6
Context Handler Owner	The manager for the CH that establishes CH rules for use by the CH. <i>Note: The CH Owner is most often the ACM Owner or the Object Owner, but may be fulfilled by an enterprise entity that manages all CHs for an enterprise.</i>	
Context Handler Rules	Rules that designate the sequence, location, handling requirements, and other external interface and internal logical functions of an ACM. <i>Note: CH rules can be encapsulated within the object attributes, the applicable DP for a given object, or pre-provisioned to the CH as a set of DPs.</i>	
Digital Policy	A policy to be enforced by a system that is encoded in such a way that it can be interpreted and enforced by an enterprise system in an automated way, i.e., without human intervention.	3

Term	Definition	Reference
Digital Policy Management	The act of dynamically creating, disseminating, and maintaining hierarchical rule sets to control digital resource management, utilization, and protection.	3
Digital Policy Management Framework	A conceptual structure intended to serve as a guide for developing systems, standards, and technologies that implement DPM functions for ABAC policies. <i>Note: See Framework definition.</i>	
Digital Policy Revocation List	The mechanism through which outdated, erroneous, or otherwise deactivated policies are captured. <i>Note: A DPRL works similar to Certificate Revocation Lists in a public key infrastructure where DPM components evaluate the DPRL to determine whether the DP being used has been revoked prior to using it.</i>	
Digital Policy Revocation Service	A service provided by the system entity that acts as the authoritative source of a DPRL.	
Digital Policy Synchronization Manager	An entity that manages dissemination, update, and revocation of enterprise—or hierarchically managed and distributed—DPs.	
Enterprise	An organization with a defined mission or goal and a defined boundary, using information systems to execute that mission, and with responsibility for managing its own risks and performance. <i>Note: An enterprise may consist of all or some of the following business aspects: acquisition, program management, financial management (e.g., budgets), HR, security, information systems, and information and mission management.</i>	3
Enterprise Policy Retrieval Point	The conduit through which enterprise policies are provisioned to the local PRPs.	
Environmental Condition Attribute Retrieval Point	A type of PIP that acts as a source of ECA values.	
Extensible Access Control Markup Language	An OASIS standard that describes both a policy language and an access control decision request and response language [both written in eXtensible Markup Language (XML)].	10
Framework	A real or conceptual structure intended to serve as a support or guide for the building of something useful.	1
Human-Readable Structured Language Policy	A policy written in a format that (a) can be read and understood without structured-language training and (b) uses available attributes in a constrained syntax that can be automatically translated to or from DP without human intervention.	
Identity	The set of attribute values (i.e., characteristics) by which an entity is recognizable and that, within the scope of an identity manager's responsibility, is sufficient to distinguish that entity from any other entity.	3
Identity Management	The combination of technical systems, policies, and processes that create, define, govern, and synchronize the ownership, utilization, and safeguarding of identity information.	3
Object Attribute Retrieval Point	A type of PIP that acts as a source of object attribute values.	
Obligation	An operation specified in a rule, policy, or policy set that should be performed by the PEP in conjunction with the enforcement of an authorization decision.	6

Term	Definition	Reference
Obligation Target	The entity to which the CH must pass any authorization obligations for fulfillment. <i>Note: The OT could be an object, an external obligation management service, or another entity.</i>	
Personally Identifiable Information	Information that can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc., alone or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.	11
Policy	A set of rules, an identifier for the rule-combining algorithm, and (optionally) a set of obligations or advice. <i>Note: May be a component of a policy set.</i>	6
Policy Administration	The process of creating, disseminating, modifying, managing, and maintaining hierarchical rule sets to control digital resource management, utilization, and protection in a standard policy exchange format.	3
Policy Administration Point	The system entity that creates a policy or policy set.	6
Policy-combining Algorithm	The procedure for combining the decision and obligations from multiple policies.	6
Policy Decision Point	A system entity that makes authorization decisions for itself or for other system entities that request such decisions.	3
Policy Enforcement Point	A system entity that requests and subsequently enforces authorization decisions.	3
Policy Information Point	The system entity that acts as a source of attribute values.	6
Policy Retrieval Point	The system entity that acts as a source of Activated DP rules.	
Policy Set	A set of policies, other policy sets, a policy-combining algorithm, and (optionally) a set of obligations or advice. <i>Note: May be a component of another policy set.</i>	6
Provenance	A record that describes entities and processes involved in producing and delivering or otherwise influencing an information resource.	6
Retired DP	DP that was Activated DP and has been removed from the set of DPs used in policy enforcement due to its being revoked, replaced (updated), or expired.	
Rule	A component of a policy that includes a target, an effect, a condition, and (optionally) a set of obligations or advice.	6
Rule-combining Algorithm	The procedure for combining decisions from multiple rules.	6
Subject Attribute Retrieval Point	A type of PIP that acts as a source of subject attribute values.	
Verified DP	DP that was Approved DP and has been deemed appropriate for dissemination and sharing after being assessed along with previously Verified DPs for potential conflicts and synergistic effects of policy combining.	