



Privacy, Access and Security Services (PASS)

Access Control Services

Conceptual Model

Draft Standard for Trial Use Ballot

Release 1.0

First Ballot

January 2010

| | |
|---------------------------------|--|
| PASS Alpha Project Lead | Don Jorgenson (Inpriva, Inc.) mailto:djorgenson@inpriva.com |
| PASS Alpha Project Coordinators | Tracy Page (Page Consulting) mailto:pageconsulting@gmail.com Gila Pyke (Cognaisance Inc.) mailto:gila@pyke.ca |
| Authors | Patrick Pyette (Perimind) mailto:patrick.pyette@perimind.com Mike Davis (Veterans Health Administration) mailto:Mike.Davis@va.gov Ed Coyne (Veterans Health Administration) mailto:Ed.Coyne@va.gov Don Jorgenson (Inpriva) mailto:djorgenson@inpriva.com |

Preface

Note to Readers

This document contains the Conceptual Model for the PASS-Access Control Service. The document supports the HL7 Services Aware Enterprise Architecture Framework (SAEAF), under which this project is governed. Further context is given in the overview section below, but one key point to note is that this specification encompasses at the conceptual level, all of the viewpoints identified by the SAEAF.

The Informational Viewpoint section of this document references previous and concomitant work from the Composite Privacy Domain Analysis Model (DSTU) and Security Domain Analysis Model (January 2010 Ballot).

It is critical to note that this specification is NOT the specification of a service, document, or messaging implementation; rather it is an unconstrained conceptual specification of the domain material.

Changes from Previous Versions

The following is a summary of changes from previous versions:

- Initial version – no changes

Acknowledgements

This ballot was developed with support from the Substance Abuse and Mental Health Services Administration (SAMHSA) and the Department of Veteran's Affairs (VA). In addition to the listed authors, the following individuals are acknowledged for their contributions during the development of this document, or previous versions that formed the basis for this document:

Laura Bright (Bell Canada)

<mailto:laura.bright@bell.ca>

Steven Connolly (Apelon)

<mailto:sconnolly@apelon.com>

Rob Horn (AGFA)

<mailto:robert.horn@agfa.com>

Suzanne Gonzales-Webb (Veterans Health Administration)

<mailto:suzanne.l.gonzales-webb@saic.com>

Steven Meyer

<mailto:smeyer@computer.org>

John Moehrke (GE Healthcare)

<mailto:John.Moehrke@med.ge.com>

Cliff Thompson (Onto Solutions)

<mailto:cliff@ontosolutions.com>

Richard Thoreson (SAMHSA)

<mailto:richard.thoreson@samhsa.hhs.gov>

Table of Contents

| | | |
|----------|---|-----------|
| 1 | INTRODUCTION | 1 |
| 1.1 | SCOPE | 2 |
| 1.2 | STATEMENT OF NORMATIVE COMPONENT | 2 |
| 2 | BUSINESS VIEWPOINT (INFORMATIVE) | 3 |
| 2.3 | OVERVIEW | 3 |
| 2.4 | BUSINESS MODEL | 3 |
| 2.5 | SCENARIOS..... | 6 |
| 2.5.1 | <i>Actors</i> | 6 |
| 2.5.2 | <i>Record access</i> | 6 |
| 2.5.3 | <i>Break Glass</i> | 6 |
| 2.5.4 | <i>Emergency Access</i> | 7 |
| 2.5.5 | <i>Emergency Access - Delegation</i> | 7 |
| 2.5.6 | <i>Emergency Access - Individual</i> | 7 |
| 2.5.7 | <i>Emergency access / Network-wide</i> | 8 |
| 2.5.8 | <i>Information is withheld from patient</i> | 8 |
| 2.6 | USE CASES..... | 9 |
| 2.6.1 | <i>Assumptions</i> | 10 |
| 2.6.2 | <i>Use Case AC-1: Enforce Access Control Decision</i> | 11 |
| 2.6.3 | <i>Use Case AC-2: Request Access Control Decision</i> | 12 |
| 2.6.4 | <i>Use Case AC-3: Submit Policy</i> | 12 |
| 2.6.5 | <i>Use Case AC-4: Submit Audit Record</i> | 13 |
| 2.6.6 | <i>Use Case AC-5: Request Policy</i> | 14 |
| 2.6.7 | <i>Use Case AC-6: Request Attributes</i> | 14 |
| 2.6.8 | <i>Use Case AC-7: Manage Policy</i> | 15 |
| 2.6.9 | <i>Use Case AC-8: Send Policy</i> | 16 |
| 2.7 | HEALTHCARE ACCESS CONTROL REQUIREMENTS | 17 |
| 3 | INFORMATIONAL VIEWPOINT | 22 |
| 3.1 | BUSINESS RULES / CONSTRAINTS..... | 22 |
| 3.2 | INFORMATION MODEL | 22 |
| 3.2.1 | <i>Security Policy Information Model</i> | 23 |
| 3.2.2 | <i>Privacy Policy Information Model</i> | 24 |
| 3.2.3 | <i>Consent Directive Information Model</i> | 25 |
| 3.3 | SEMANTIC SIGNIFIERS (NORMATIVE)..... | 25 |
| 3.3.1 | <i>Access Request Message</i> | 26 |
| 3.3.2 | <i>Policy Selection Criteria</i> | 28 |

| | | |
|----------|--|-----------|
| 3.3.3 | <i>Access Control Policy</i> | 29 |
| 3.3.4 | <i>Attribute Selector (Informative)</i> | 29 |
| 3.3.5 | <i>Privacy Policy and Consent Directive</i> | 30 |
| 3.3.6 | <i>Access Control Decision (Informative)</i> | 30 |
| 3.3.7 | <i>Policy Management Request</i> | 31 |
| 3.3.8 | <i>Policy Management Response</i> | 32 |
| 3.4 | DYNAMIC MODEL | 33 |
| 4 | COMPUTATIONAL VIEWPOINT | 35 |
| 4.1 | OVERVIEW | 35 |
| 4.2 | CAPABILITIES | 35 |
| 4.2.1 | <i>Enforce Access Control Decision</i> | 35 |
| 4.2.2 | <i>Request Access Control Decision</i> | 36 |
| 4.2.3 | <i>Get Access Decision Information</i> | 37 |
| 4.2.4 | <i>Get Policy</i> | 38 |
| 4.2.5 | <i>Submit Access Control Policy</i> | 39 |
| 4.2.6 | <i>Submit Audit Record</i> | 40 |
| 4.2.7 | <i>Manage Policy</i> | 41 |
| 4.3 | COLLABORATION ANALYSIS | 42 |
| 4.3.1 | <i>Access Control</i> | 42 |
| 4.3.2 | <i>Policy Management</i> | 45 |
| 4.4 | CONFORMANCE (NORMATIVE) | 46 |
| 4.4.1 | <i>Contracts</i> | 46 |
| 4.4.2 | <i>Conformance Profiles</i> | 50 |
| 5 | ENGINEERING VIEWPOINT | 53 |
| 5.1 | ODP FUNCTIONS | 53 |
| 5.1.1 | <i>Physical Distribution Functions</i> | 53 |
| 5.1.2 | <i>Communication Functions</i> | 53 |
| 5.1.3 | <i>Processing Functions</i> | 53 |
| 5.1.4 | <i>Storage Functions</i> | 53 |
| 5.2 | ENGINEERING ROLES | 53 |
| 6 | APPENDIX A - GLOSSARY OF TERMS | 54 |
| 7 | APPENDIX B - RELATED STANDARDS | 57 |

List of Illustrations

| | |
|--|----|
| ILLUSTRATION 1 GENERALIZED ACCESS CONTROL MODEL | 3 |
| ILLUSTRATION 2 AUTHORIZATION REFERENCE MODEL | 5 |
| ILLUSTRATION 3 BOUNDARY VIEW OF THE ACCESS CONTROL SERVICE | 9 |
| ILLUSTRATION 4 POLICY MANAGEMENT BOUNDARY VIEW | 10 |
| ILLUSTRATION 5 SECURITY POLICY INFORMATION MODEL (EXTRACTED FROM SECURITY DOMAIN ANALYSIS MODEL – INFORMATIONAL BALLOT - JANUARY 2010 | 23 |
| ILLUSTRATION 6 PRIVACY POLICY INFORMATION MODEL (EXTRACTED FROM COMPOSITE PRIVACY DOMAIN ANALYSIS MODEL – DSTU – SEPTEMBER 2009) | 24 |
| ILLUSTRATION 7 CONSENT DIRECTIVE INFORMATION MODEL (EXTRACTED FROM COMPOSITE PRIVACY DOMAIN ANALYSIS MODEL – DSTU – SEPTEMBER 2009) | 25 |
| ILLUSTRATION 8 ACCESS REQUEST MESSAGE | 26 |
| ILLUSTRATION 9 POLICY SELECTION CRITERIA | 28 |
| ILLUSTRATION 10 ATTRIBUTE REQUISITIONING AND PROVISIONING | 30 |
| ILLUSTRATION 11 POLICY DECISION AND OBLIGATIONS | 31 |
| ILLUSTRATION 12 POLICY MANAGEMENT REQUEST | 32 |
| ILLUSTRATION 13 POLICY MANAGEMENT RESPONSE | 33 |
| ILLUSTRATION 14 POLICY CONCEPTUAL LIFECYCLE | 34 |
| ILLUSTRATION 15 ACCESS CONTROL ROLES AND CAPABILITIES | 43 |
| ILLUSTRATION 16 CAPABILITY COLLABORATIONS FOR ENFORCE POLICY DECISION | 44 |
| ILLUSTRATION 17 POLICY MANAGEMENT ROLES AND CAPABILITIES | 45 |
| ILLUSTRATION 18 - CONFORMANCE PROFILE: ACCESS CONTROL SERVICE 1 | 50 |
| ILLUSTRATION 19 - CONFORMANCE PROFILE: ACCESS CONTROL DECISION 1 | 50 |
| ILLUSTRATION 20- CONFORMANCE PROFILE: ACCESS CONTROL DECISION 2 | 51 |
| ILLUSTRATION 21 - CONFORMANCE PROFILE: ADI PROVISIONER | 51 |
| ILLUSTRATION 22 - CONFORMANCE PROFILE: AC POLICY PROVISIONER | 52 |

1 Introduction

The purpose of this document is to describe the conceptual-level viewpoints associated with the business requirements that relate to the content, structure, and functional behavior of information important to the Access Control area of the Privacy, Access, and Security domains within the healthcare environment.

This document seeks to define the business requirements of an Access Control service. This document comprises the four viewpoints identified by the HL7 Services Aware Enterprise Architecture Framework (SAEAF) at the conceptual level: Business, Informational, Computational, and Engineering.

The goal of all SAEAF artifacts is to ensure “working interoperability”(WI) between implementations, whether they be document-, message-, or service-based. The concept of working interoperability can be described as “the deterministic exchange of data/information in a manner that preserves shared meaning”. Starting at the conceptual level (this document), the goal is to ensure that specifications are “implementable in a variety of deployment contexts, in a repeatable, comprehensible manner”. The explicit specification of any transform that may be required to allow interoperability between implementations is one of the keys to WI.

The Business viewpoint identifies the business context and scoping for the specification and contains the following artifacts:

- The use cases and scenarios that have been used to scope the work;
- A set of traceable requirements – informational, functional, and non-functional that have been extracted from the use cases and scenarios, or driven out from subsequent analysis.
- A business object model that identifies objectives and business entities, including the roles that those entities have in executing processes to achieve the stated objectives.

The Informational Viewpoint presents the object model representing the unconstrained information requirements of the system – the major entities and their relationships to each other. This viewpoint also identifies vocabulary concepts that are appropriate for the domain. Artifacts in this viewpoint include:

- A static model, containing the information objects and invariant schema
- A dynamic model, identifying allowable state changes to the information objects.

Note: This document makes reference to the parallel work sponsored by the HL7 Security WG which is tasked with producing a Security Domain Analysis Model (DAM). The Security DAM focuses on the information artifacts required to communicate and execute policies for access control and authorization. The PASS Access Control work leverages that work wherever possible. This document’s focus in this regard will be on filling any gaps that result from our analysis of functional behavior.

Additional reference in the Informational Viewpoint is made to the Community-Based Collaborative Care (CBCC) – Composite Privacy Domain Analysis Model (DSTU), which was balloted in September 2009.

The Computational viewpoint presents the functional behavior of an Access Control Service grouped so that they are distributable and may be exposed through service interfaces.. It documents the collaboration analysis performed, identifies service roles and responsibilities, and groups the service

capabilities and operational semantics into contracts and profiles.

The Engineering viewpoint identifies and captures any relevant platform capabilities, and documents any essential requirements for the distribution of any of the functionality identified.

1.1 Scope

This document presents the information and capabilities required to provide Access Control services to protected resources in a distributed healthcare environment, where interoperability requirements arise.

A pre-requisite to any Access Control activity is the management of Access Control policies. This document considers the behavior associated with the lifecycle of those policies.

While identified in the document, the capabilities and semantic information associated with informational Consent Management and Client Privacy Policy Management (identified in the document as Interfaces 3 and 4 respectively) are specifically set out of scope. Subsequent work will be required to elaborate the remaining interfaces.

1.2 Statement of Normative Component

The majority of behavior identified in the Access Control business domain is not healthcare specific, and therefore cannot be considered as normative content.

What can be considered normative are the following items:

1. The semantic content unique to healthcare in the Access Control business domain.
2. The specific contracts which result from combining behavior with the semantic content identified above.
3. The conformance profiles, which group specific contracts into service components at the conceptual level.

2 Business Viewpoint (Informative)

2.3 Overview

Identified within the Business Viewpoint are the business issues, models, processes, and roles associated with the Access Control sub-domain of Privacy, Access, and Security Services.

2.4 Business Model

The concepts of the control model as identified in ISO TS 22600-2:2006, Privilege Management and Access Control – Part 2: Formal Models, are extended in this document. The illustration below is a representation of the control model put forward in that document.

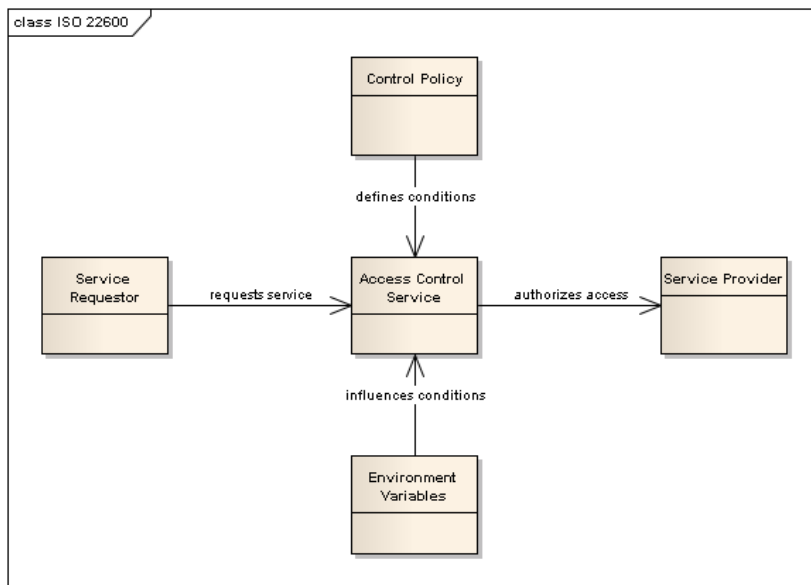


Illustration 1 Generalized Access Control Model

The Service Requestor has certain privilege attributes provided by an authority that is trusted by the Access Control Service. The Service Provider is a protected resource with certain attributes that influence the selection of an appropriate Policy or the path through the policy that is applied to the request. Environment variables may provide additional factors that may impact evaluation of the policy.

When a request for service is made, the Access Control Service protects the Service Provider from unauthorized access in accordance with the Control Policy.

Illustration 2, below shows an expanded view of the Access Control Service modeled after ISO 10181-3 Access Control Framework, exposing this service in the context of its generalized access control information types (per ISO) and associated Service Provider Security and Consent Management activities. Since the model is a general one, it applies to any number of verticals/industries and is in itself not healthcare specific. In particular, there is no component that is explicitly limited to a healthcare environment. The possibility for healthcare specific concerns exists only in the four interfaces: Service Consumer to Policy Enforcement Point (PEP) interface; Policy and Access Control

Information (ACI) stores interface; Consent Management interface, and Patient Privacy Policy interface.

Within the Authorization Reference Model four interfaces are identified:

- Interface 1, is the Service Consumer to PEP interface. It is healthcare specific through the Access Decision Information (ADI) contained in the request. This interface includes the service consumer request including asserted access control attributes (ADI) that are intercepted by the Service Provider Access Control Service. Service Consumer ADI along with Resource and any retained Service Consumer (e.g. Subject ADI) and associated Contextual information is provided to the Policy Decision Point (PDP) to be combined with relevant security and privacy rules in order to make an access control decision. This interface has been described in one instance as a SAML Attribute Assertion with a US specific Profile.
- Interface 2 is the policy and ACI stores. Interface 2 is the interface of the data stores shared by Security Management and the ACS. These policies are “owned” by Security Management and consumed by the ACS. The content of these stores contain healthcare specific policy references and healthcare ACI/ADI value sets. There is, however, nothing specific about these policy stores that warrant a healthcare specific mechanism to provision or access their information.
- Interface 3 is the Consent Management interface. This interface conveys authoritative organization agreed-to patient privacy policy to the Security Management layer. This is interpreted as privacy policies accepted and agreed to by the Service Provider to Security Management for integration into the Service Provider’s composite Security and Privacy Policy store. This could represent automated inclusion of certain pre-agreed to policies (e.g. Opt-in to Health Information Exchange (HIE) participation) or a manual process.
- Interface 4 is the Personal Privacy Policy interface. Interface 4 can convey either:
 - An external organization agreed-to Client privacy policy that they have accepted, or
 - A PHR-sourced Client privacy policy for consumption by this Service Provider’s Privacy Management layer and possible acceptance as agreed-to Client privacy policy for enforcement.

Consent Management provides the means to deal with Client privacy policies received from the outside, reflecting input from a Service Consumer, another Service Provider or from a Personal Health Record. Such policies are permitted, but may require additional scrutiny and Privacy Management oversight in order to determine Service provider acceptance or agreement prior to placing in the directory of Privacy Policies.

The interleaving Security Management layer represents that portion of the Service Provider’s internal management processes that links Client privacy policy (from Consent Management) with Service Provider (organizational and jurisdictional) privacy policies. Security Management bears overall responsibility for the management of organizational security and privacy policies, provisioning of Resource and Subject ACI and associated Contextual information, Privilege Management, Identity and Access Management, and all other activities surrounding the maintenance and operation of the Service Provider’s authoritative secure access control information base.

Within the Security Management layer, personal privacy policy references in the Privacy Policy directories are mapped to ACS-executable privacy policy/policy sets. Security Management prepares Client-originated policies (agreed to by the Service Provider) for linking to existing policy rules and constraints. It is in the Security Management layer that Consumer Privacy Policies are bound to existing

organizational and jurisdictional privacy policies to create the complete composite policy/policy sets that will be called upon in the context of a specific request by a Service Consumer. Security management is a critical function in preparing and provisioning ACI for ACS use.

Note: Illustration 2 is not meant to imply that a one-to-one relationship exists between a Policy Decision Point and a Policy Enforcement Point. A Policy Decision Point may perform that role for multiple Policy Enforcement Points.

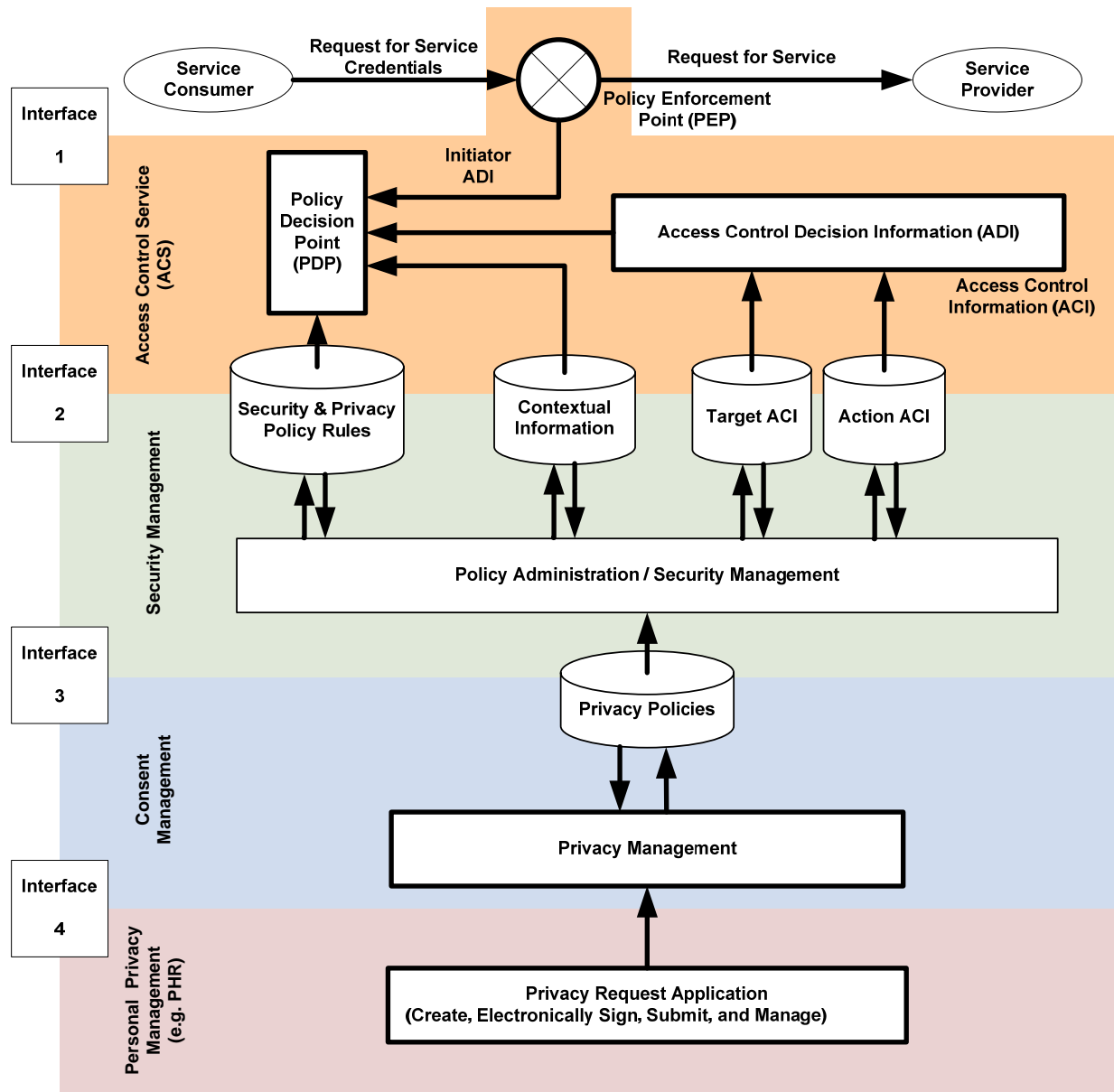


Illustration 2 Authorization Reference Model

2.5 Scenarios

During our business analysis, we examined a number of healthcare-specific scenarios that were thought to have Access Control implications. The scenarios below expose some specific semantic or behavioral aspect of the service in a healthcare environment.

2.5.1 Actors

| | |
|----------------------|---|
| Adam Everyman | a Patient |
| Eve Everywoman | a Patient |
| Dr. Patricia Primary | a primary care physician in a group practice. |
| Dr. Serena Shrink | a psychiatrist with Doctor's Unlimited |
| Nancy Nightingale | a nurse working in Dr. Shrink's office |
| Dr. Eric Emergency | an emergency room physician with Good Health Hospital |
| I.T. Admin | a system administrator at Good Health Hospital |

2.5.2 Record access

Adam recently has started visiting Dr. Shrink for treatment of a generalized anxiety disorder and obsessive compulsive disorder. He is sensitive about this information being widely known and asks that information about his visits and treatment there be restricted to the care team at Dr. Shrink's office. Dr. Shrink agrees and sets up the constraints in his EMR. Dr. Shrink sends Adam for some preliminary blood work and prescribes a medication. Both actions and the lab results are stored in the system.

A week later, Adam visits Dr. Primary, his primary care physician for a routine visit. She logs in to her EMR system to review Adam's record.

Results of tests previously ordered by her clinic are displayed, as are results from Adam's physiotherapy, and a visit to a bone fracture clinic for treatment of a hockey injury last year. As a result of the constraints set up by Dr. Shrink, treatment information from Dr. Shrink's clinic and the associated medication record are not returned. Depending on jurisdictional or organizational privacy policies, Dr. Shrink may or may not be notified that some information may be missing.

2.5.3 Break Glass

Break-glass is named after the glass panel that protects a fire alarm. Everyone in the building is authorized to use the fire alarm to report a fire, but the ramifications of misuse are substantial. The fragile glass panel is sufficient to avoid accidental triggering, and it forces the user to stop and think before acting.

In the context of this document, a "Break Glass" scenario involves a situation where the access control policy will authorize the user to access certain information or functionality, but only after the user attests that one or more relevant conditions exist.

Assumptions:

- Execution of the “break glass” function results in a request to the Access Control Service and includes the “break glass” context information.

Eve Everywoman is going through a divorce from her husband, Dr. Patrick Pump and is fighting for custody of her children. She fears that if her husband learns about her current treatment for anxiety and depression, he will use this against her somehow. She knows that his position as a physician and his numerous medical contacts at the clinic she visits make it easy for him to find out about her treatment. She asks the clinic to institute a consent directive whereby she restricts the use and disclosure of all of the information collected by clinic by anyone.

When Eve next visits the clinic, Serena Shrink is unable to access any of Eve’s records that did not originate with Dr. Shrink. Eve consents to the disclosure of those records to Dr. Shrink. The physician then invokes the 'break glass' function, enters the fact that the patient has verbally consented to the action for the purpose of treatment during this encounter and submits the request. The previously hidden results now appear on her monitor.

When Dr. Shrink invokes the “break glass” function, the audit service is invoked, potentially triggering an alert mechanism. This is an important deterrent to those who might otherwise “break the glass” without reasonable cause. The audit service is also critical to providing elements of such things as access and disclosure reporting.

2.5.4 Emergency Access

There are a number of types of Emergency access. In some jurisdictions, emergency access is considered to be a purpose of use, while in others it is an environmental attribute to be considered. These scenarios are here for completeness, however only administrative interfaces may be affected. In no case is additional interoperable behavior expected of the service.

2.5.5 Emergency Access - Delegation

There is a major traffic disaster on the Eisenhower Expressway. Most of the administrative staff are able to get into the hospital that morning, but only one doctor, Eric Emergency, is able to get to the ED (Emergency Department). Eric is able to see all of the patients, but not able to see them and document orders in the computer in a timely fashion. In order to ensure that orders are entered appropriately, the administrative staff are “deputized” to enter the orders as he calls them out.

2.5.6 Emergency Access - Individual

Eric Emergency is the only emergency physician working the graveyard shift in a small rural hospital and has forgotten his password. The system administrator is unavailable to reset Eric's password until morning. Eric will be unable to be effective as a physician without access to the computers.

A procedure may be in place that temporarily allows a physician access based on other identification criteria. For example, a sealed envelope with ID and password may be kept in a locked cabinet. Nancy Nightingale is authorized to counter-sign its use and activate it for Eric, based on personal knowledge that this is Eric.

2.5.7 Emergency access / Network-wide

Assumptions:

- Policies exist that allows elevated access when an emergency is indicated. No explicit interaction with the requesting user is required.
- Auditing requirements will be policy-dependent.
- Network wide emergencies often are associated with selective loss of individual systems and communications links. Power loss typically triggers automatic shutdown of non-critical loads. If the power loss is expected to be lengthy, all systems other than those needed to sustain care may be shut down. These shutdowns often result in loss of portions of the security infrastructure. Therefore, the need for emergency access also includes managing alternative access controls.

A hurricane has resulted in massive flooding, damage to roads, communication lines, etc., and a significant increase in illness and injuries requiring emergency treatment.

All healthcare facilities in the affected area respond by bringing in all available providers from external agencies to augment medical staff. External providers are provisioned on the security system. They are also granted standard accesses that will allow them to operate including the ability to adopt an Emergency Role.

2.5.8 Information is withheld from patient

Assumptions:

- Adam has an agreement with Dr. Primary's clinic which allows the clinic to disclose any of Adam's health information, deemed appropriate by the clinic, to Adam's PHR.
- The jurisdiction in which Dr. Primary practices provides her with the authority to determine what, if any, medical information should be disclosed to the patient.

Dr. Primary receives the results of some of the lab tests that she ordered for Adam, which contain information that she believes could be harmful to Adam's well being if Adam was not informed of the results in an appropriate manner. Dr. Primary marks this information as not to be disclosed to the patient.

During the nightly download of information from the clinic's EMR system to Adam's PHR, all of Adam's information is disclosed to the PHR, with the exception of the information previously marked as not to be disclosed.

2.6 Use Cases

The use cases presented below reflect those identified during the initial phase of the PASS ACS project work. The boundary diagrams below illustrate the relationships that the Access Control Service and the Policy Management Service have with their external stakeholders and each other.

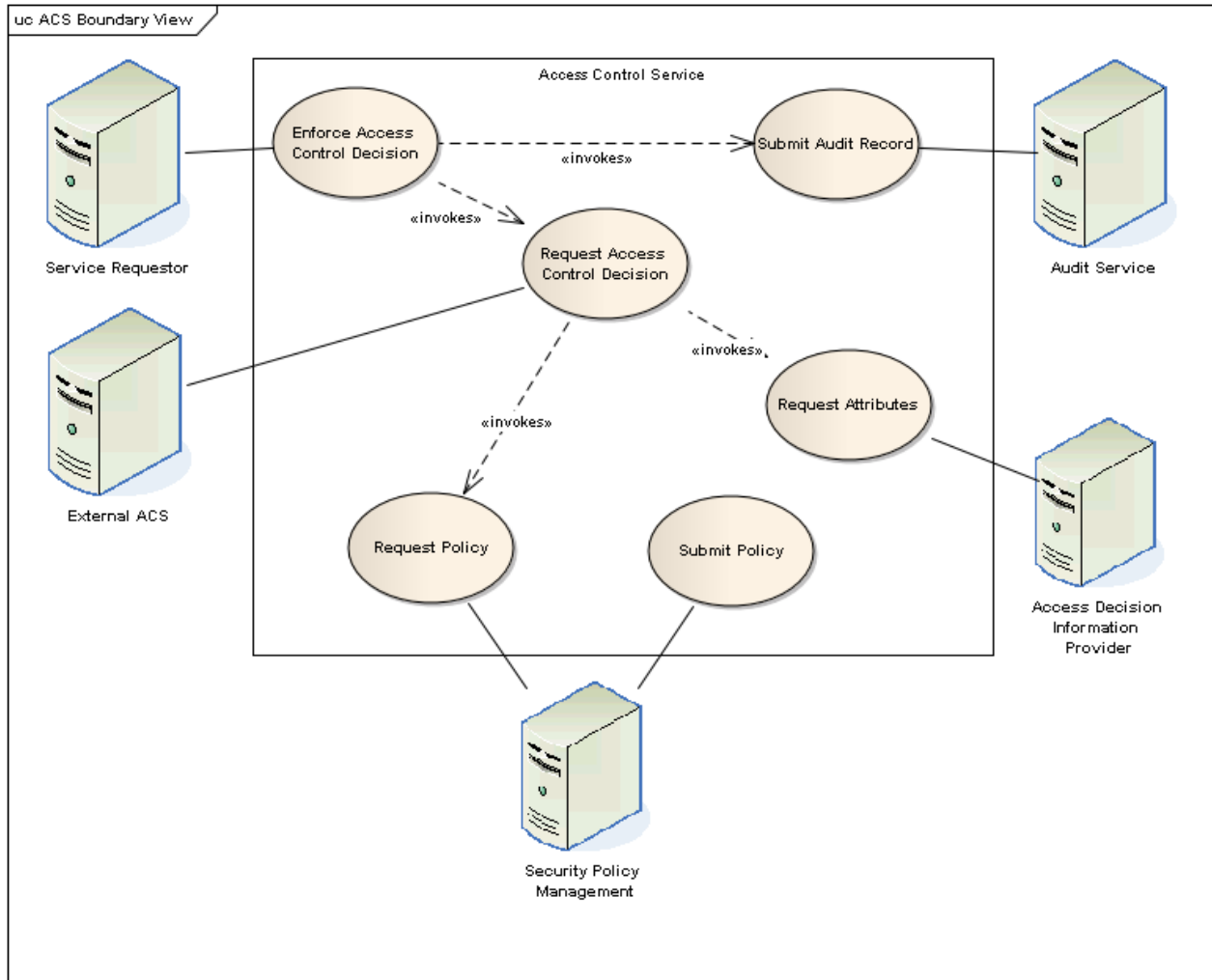


Illustration 3 Boundary View of the Access Control Service

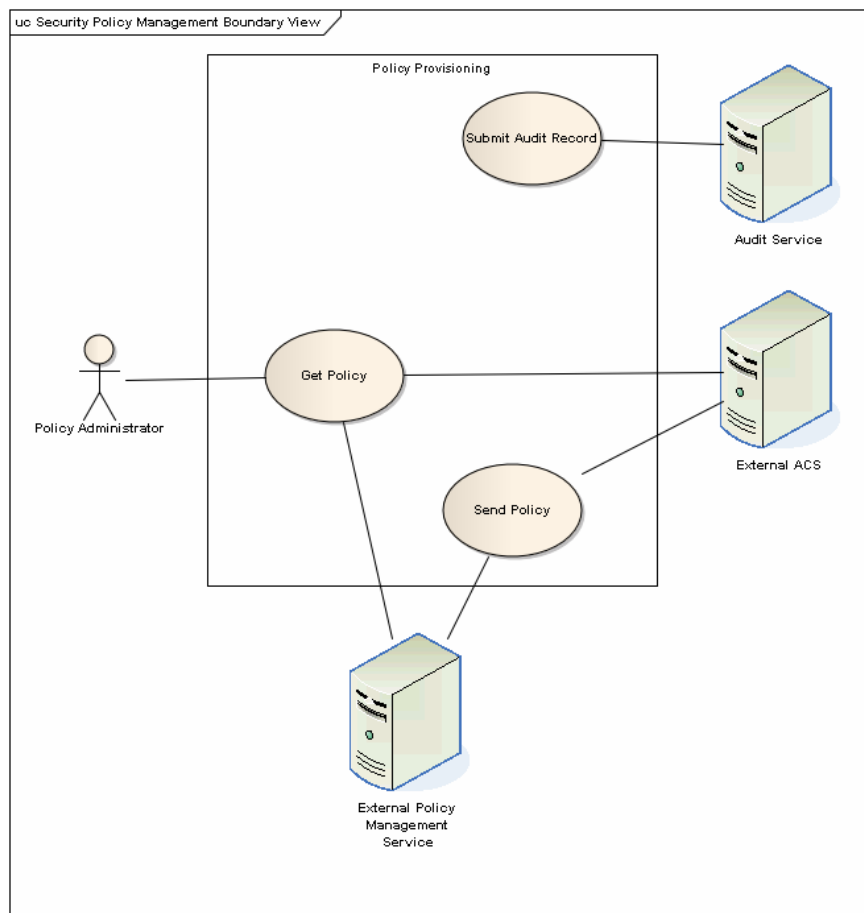


Illustration 4 Policy Management Boundary View

2.6.1 Assumptions

Multiple architectural styles supported

This analysis requires that a number of different mechanisms for policy retrieval and reference be considered. The issue is especially relevant when looking at evaluating Privacy Policies with Client-specific attributes.

As an example, a base Privacy Policy may indicate that a Client can withdraw their consent to the disclosure of their Individually Identifiable Health Information (IIHI) from all but an identified list of providers or organizations. The Consent Directive is an instance of that policy, with real values for that list (or no values at all).

We have identified at least four different architectural mechanisms that may be needed for resolving the Client's consent directive, and at the conceptual level, will need to ensure that all four can be supported. These four mechanisms are:

- Each Consent Directive is executable and makes up part of the authoritative Access Control policy store. Consent Directives are evaluated as any other Security or Privacy policy would be.
- The base policy is constructed in such a way as to refer to an attribute obtained by the

invocation of an external policy decision point which holds the Client's directives.

- The Access Control Service requests the executable Consent Directive from a trusted policy provisioning agent.
- The base Policy is constructed such that the required list of providers or organizations is retrieved as Access Control Decision Information (ADI) from a Privacy Policy or Consent Directive source.

Distributed Capabilities

There is an assumption that any of the identified capabilities or use cases may be distributed. The exercise of creating conformance profiles will determine the most appropriate "packaging" of behavior. Where applicable, each of the use cases is based on the assumptions of two domains: Domain "A" and Domain "B", with distinct access control policies, but which participate in a shared identity federation.

2.6.2 Use Case AC-1: Enforce Access Control Decision

Description

Invoke a function to decide whether to allow access to a resource based upon currently active policies and ensure that the decision is enforced, logging the results.

Assumptions

- Each request contains a set of Requestor attributes including:
 - A unique identity
 - A set of authorization claims or credentials, which can be validated
 - A set of attributes which provide additional context for the request. These attributes may include, but are not limited to:
 - The intended purpose of use which the Requestor has for the resource(s);
 - Whether the request is a "break-glass" request;
 - Whether an emergency condition exists, etc.
- Each request contains a mechanism to uniquely identify the resource(s) that are the target of the request.
- Each request contains the operation that is being requested to be performed on the resource(s).

Actors

Service Requestor (via a Protect Resource or its supporting infrastructure)

Trigger Event

The use case is triggered when a request is issued to access a Protected Resource

Pre-conditions

- Two security domains exist (Domain A and Domain B). Security Domains are defined as separate entities each with a set of subjects and information objects, and a common security policy (NIST Special Publication 800-33).

- A trust relationship exists between Domain A (Security Domain A) and Domain B (Security Domain B).

Post-conditions

The requested operation has either been permitted or denied.

2.6.3 Use Case AC-2: Request Access Control Decision

Description

Provide an access control decision, based on access control policy evaluation of an incoming request to perform a specified operation on a Protected Resource.

Assumptions

- See AC-1: Enforce Access Control Decision assumptions

Actors

- Service Requestor indirectly

Trigger Event

The use case is triggered by UC-1: Enforce Access Control Decision

Pre-conditions

- A policy, applicable to the request, exists and is available to the decision function.

Post-conditions

- An access control decision has been rendered, along with any obligations associated with the decision.

2.6.4 Use Case AC-3: Submit Policy

Description

A Policy is provided from a trusted policy source to be integrated into the operational policy store. The policy is assumed to have been through a harmonization process prior to submission.

Assumptions

- The operational policy store is contained within the Access Control Service and not within a Policy Management component.

Actors

- Policy Management

Trigger Event

The Policy Management actor presents a policy to be integrated into the operational policy store.

Pre-conditions

- A trusted policy source is available.

Post-conditions

- The policy has been integrated into the operational policy store.

2.6.5 Use Case AC-4: Submit Audit Record¹

Description

An audit event record is created and submitted to an audit repository.

Assumptions

- No assumption regarding timing is made. The audit information may be cached locally prior to transmission or transmitted upon creation.

Actors

- Service Requestor (indirect)
- Audit Service (secondary)

Trigger Event

The use case is triggered by the execution of the Enforce Access Control Decision use case.

Pre-Conditions

- An audit repository has been configured

Post-conditions

- Audit event information has been captured and transmitted to an audit repository

¹ The Submit Audit Record use case is out of scope for this PASS Access ballot and will be further detailed in a PASS Audit ballot.

2.6.6 Use Case AC-5: Request Policy

Description

A policy is requested from an external policy provisioning source.

Assumptions

- The policy provisioning source is sufficiently trusted

Actors

- Service Requestor (indirect)
- Policy Management Service (secondary)

Trigger Event

The use case is optionally triggered by the execution of the Request Access Control Decision use case.

Pre-conditions

- A trusted policy management service has been configured.

Post-conditions

- The requested policy has been retrieved and is available for evaluation.

2.6.7 Use Case AC-6: Request Attributes

Description

Requests are made to Access Decision Information Providers (external components) for Requestor (User), Resource, Client, and environment attributes associated with an access control request.

Assumptions

- Mechanisms exist that allow attribute requests to be forwarded to the correct provisioning services.

Actors

- Service Requestor (indirectly)
- Access Decision Information Provider (secondary)

Trigger Event

The use case is triggered by the execution of the Request Access Control Decision use case.

Pre-conditions

- Security and/or privacy policies exist which make reference to external Access Decision Information
- A Service Request has resulted in a policy as identified above being evaluated

Post-conditions

- The set of attributes required to evaluate the policy have been retrieved

2.6.8 Use Case AC-7: Manage Policy

Description

This use case describes the life cycle management of those executable policies evaluated in the access control decision process.

Assumptions

- There is a trust relationship between the invoking Actor and the Policy Management functions.
- The invoking Actor has the necessary authority to invoke the function.

Actors

- Policy Administrator
- External Policy Management Service
- External ACS (secondary)
- Audit Service (secondary)

Trigger Event

The use case is triggered by a Policy Administrator or external Policy Management Service wishing to modify the state of a policy.

Pre-conditions

- None

Post-conditions

- The lifecycle of the target policy has been altered.
- An audit event record has been created and will be transmitted to an Audit Service
- The target policy (with lifecycle changes applied) has been transmitted to any external Access Control Service with which the Policy Management actor has been configured to communicate.

2.6.9 Use Case AC-8: Send Policy

Description

This use case describes sending a policy to an External ACS actor.

Assumptions

- There is a trust relationship between the Policy Management function and the External ACS.

Actors

- Policy Administrator (secondary)
- External ACS

Trigger Event

The use case is triggered as part of the Manage Policy use case.

Pre-conditions

- Both the Policy Manager and the External ACS have been configured to communicate.

Post-conditions

- The target policy has been transmitted to the External ACS.

2.7 Healthcare Access Control Requirements

The table below summarizes all of the informational, functional, and quality requirements identified through review and analysis of the scenarios and use cases presented above.

Note: Where the requirements in Table 1 below identify healthcare-specific functionality or semantic content, those requirements are reflected in the Conformance section of this document.

Table 1 Access Control Requirements

| ID | Requirement Text | Responsible Service or Capability | Healthcare Specific Component ? Y/N | Functional / Semantic F/S | Implied Capability? |
|----------------------|---|-----------------------------------|-------------------------------------|---------------------------|--|
| Cross-Cutting/Global | | | | | |
| ACG-1 | Provide healthcare authorization and access control as a service. | All Layers | Y | F | |
| ACG-2 | Provide the capability to ensure that protected information is accessible only by entities possessing authorizations that meet or exceed healthcare information security and privacy policy access control decision attributes. | All Layers | Y | F/S | |
| ACG-3 | Generate security audit records based on healthcare-specific security relevant events. | All Layers | Y | S | <ul style="list-style-type: none"> - Recording security-relevant events in an audit trail - Support auditing of access control actions and administration. - The audit record produced by any service has to be conformant with the audit schema of the audit service |
| ACG-4 | Incorporate standard healthcare-specific access control information code sets per HL7 security and privacy domain models. | All Layers | Y | S | This requirement will be solved by the use of semantic signifiers as input and output parameters in the capability tables. Semantic profiles may also bind the concrete information models to |

| ID | Requirement Text | Responsible Service or Capability | Healthcare Specific Component ? Y/N | Functional / Semantic F/S | Implied Capability? |
|---------------------------------|--|-----------------------------------|-------------------------------------|---------------------------|--|
| | | | | | the semantic signifiers. |
| Interface 1 | | | | | |
| AC1-1 | Provide access control decision information (ADI, ie: policy attribute values) to another service. | Interface 1 | Y | F | |
| AC1-2 | Request access control decision information (ADI, ie: policy attribute values) from another service. | Interface 1 | Y | S | The ability to request or retrieve attributes / information / tokens / decision factors |
| AC1-3 | Provide the capability to return both a response and its associated obligation policy following a request for information. | Interface 1 | Y | S | See AC01 Obligations provide the capability to return a data use policy with the requested data. The assurance of this policy can be none, Medium (e.g. an OASIS obligation), or Strong (e.g Digital Rights Management envelope). |
| AC1-4 | Ability to request credentials from a credentialing service within or outside of ACS. | Access Control | N | F/S | May be requesting one set of services and returning another. Ability to say "I don't have enough information" but need a different credential and the type. |
| AC1-5 | Provide the capability to receive and enforce obligations associated with a return response to an information request. | Interface 1 | Y | N | The analysis and processing of Obligations are out of scope for this (January 2010) ballot. |
| Layer 1: Access Control Service | | | | | |

| ID | Requirement Text | Responsible Service or Capability | Healthcare Specific Component ? Y/N | Functional / Semantic F/S | Implied Capability? |
|--------------------|--|--|--|----------------------------------|---|
| AC1-6 | Support enforcement of any combination of healthcare-specific policies concerning subjects, resources and contexts. | Interface 1 | N | S | Flexibility to handle types of authorization policy |
| AC1-7 | Provide the capability to check if there are external policies with access control information (policy documents) that apply to the current request context. | Access Control | N | F/S | |
| Interface 2 | | | | | |
| AC2-1 | Enforce a “deny all” policy as a default. | Interface 2 | N | S | Ability to set “deny all” as a default |
| AC2-2 | Support the capability to switch preplanned profiles of policy sets based upon purpose of use. | Interface 2 | N | N | See AC 28. This can occur in different ways, e.g., input from a user that is passed as a token, input from a user that causes an invocation of a submit event capability. Use case: VoV |
| AC2-3 | Enforce security and privacy policy based on contextual, action, target or initiator access control decision information. | Interface 1 | N | S | Implement separation of duties and other policies, ie. cardinality, time of day, separation of duties, etc. |
| Interface 2 | | | | | |
| AC2-4 | Return an access control decision to another service | Interface 2 | N | F/S | Furnish an access control decision to an application or other PEP |

| ID | Requirement Text | Responsible Service or Capability | Healthcare Specific Component ? Y/N | Functional / Semantic F/S | Implied Capability? |
|-------|---|-----------------------------------|-------------------------------------|---------------------------|---|
| AC2-5 | Receive a request for an access control decision from another service | Interface 2 | N | F/S | The way you would invoke the access control decision is to say "request an access control decision" The vocabulary for these rules will come from other groups like CBCC and XSPA, and be specified in the Semantic Profile section of the SFM. Eg: - People - Roles - Intended Use - Confidentiality - Location |
| AC2-6 | Request or retrieve a policy decision from another policy decision service or access control service or other related service | Interface 2 | N | F | |
| AC2-7 | Request a machine-readable policy document from another service. | Interface 2 | Y | F/S | - Request access control info, decision factors - Request access control policies - List access control policies |
| AC2-8 | Receive a request for a machine-readable policy document from another service. | Interface 2 | Y | F | |
| AC2-9 | Support exchange of security and privacy policy documents with other access control service. | Interface 2 | Y | F | Ensure that the same policy that is distributed over more than one ACS provides the same access control results everywhere at the same point in time. This implies a number of functions: a) notification of policy updates b) distribution of updated policies (push or pull) c) synchronized policy activation / |

| ID | Requirement Text | Responsible Service or Capability | Healthcare Specific Component ? Y/N | Functional / Semantic F/S | Implied Capability? |
|--------|---|-----------------------------------|-------------------------------------|---------------------------|---|
| | | | | | deactivation |
| AC2-10 | Support enforcement of nested policy sets. | Interface 2 | N | S | May be better to have a separate result conflict resolution requirement that more clearly includes rule decision conflicts. |
| AC2-11 | Respond to a request for a machine-readable policy document from another service. | Interface 2 | Y | S | |

3 Informational Viewpoint

3.1 Business Rules / Constraints

None identified

3.2 Information Model

Information Models provide the basis for semantic content for Access Control. Previous and concomitant work has been done by other projects and is leveraged herein.

The HL7 Security Domain Analysis Model and Composite Privacy Domain Analysis Model documents are on track to become HL7 standards and are intended to become normative to this model when available. In the meantime, draft and Draft Standard for Trial Use (DSTU) UML models taken from the source material has been placed here solely for the reader's convenience. A complete copy of the Security Domain Analysis Model Informative ballot (January 2010) is appended to this document for reference.

The current Composite Privacy Consent Directive Domain Analysis Model may be found at:

http://www.hl7.org/v3ballot/html/dams/uvpr/Composite_Privacy_DAM_v1_r2.pdf

3.2.1 Security Policy Information Model

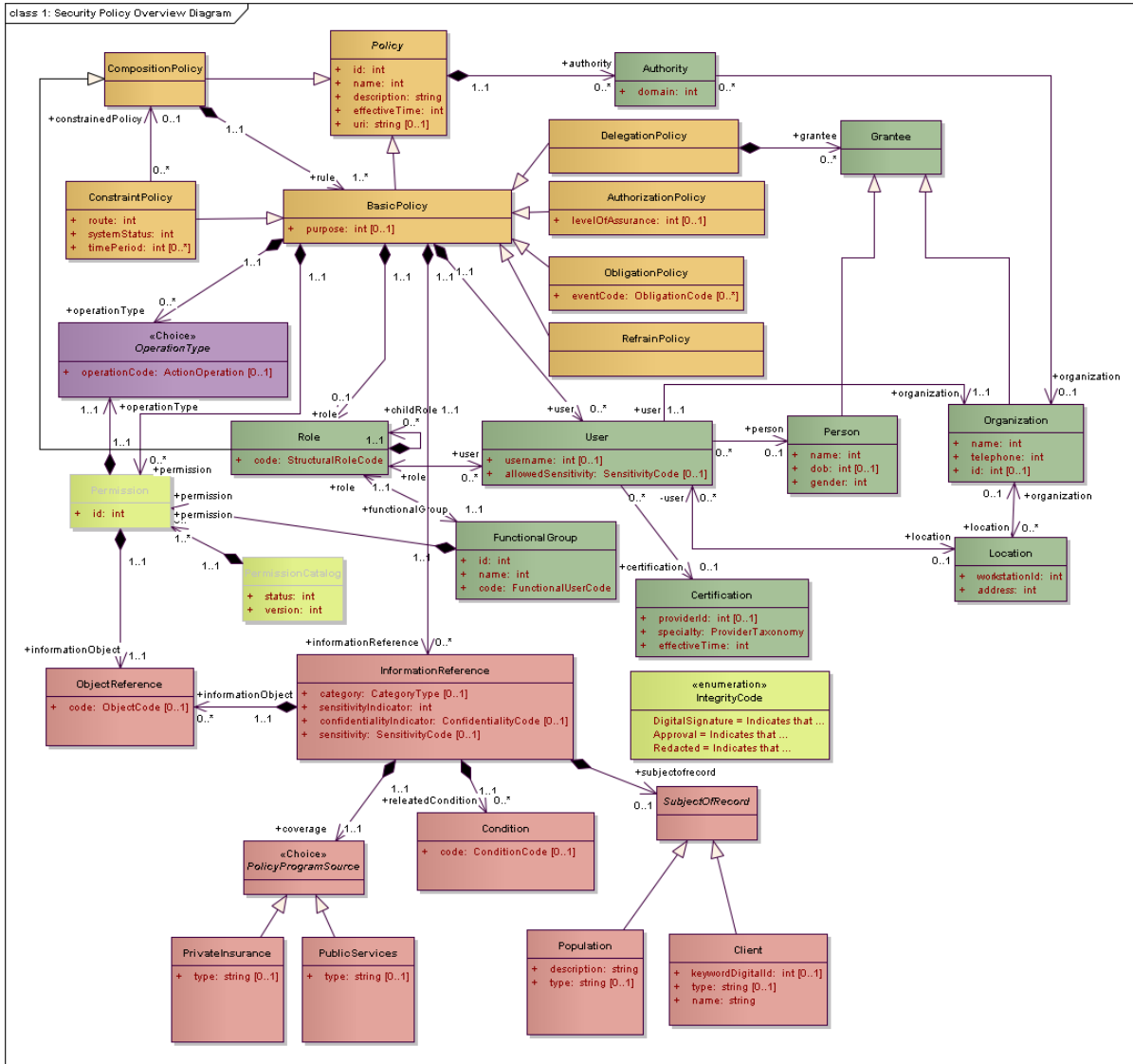


Illustration 5 Security Policy Information Model (Extracted from Security Domain Analysis Model – Informational Ballot - January 2010)

3.2.2 Privacy Policy Information Model

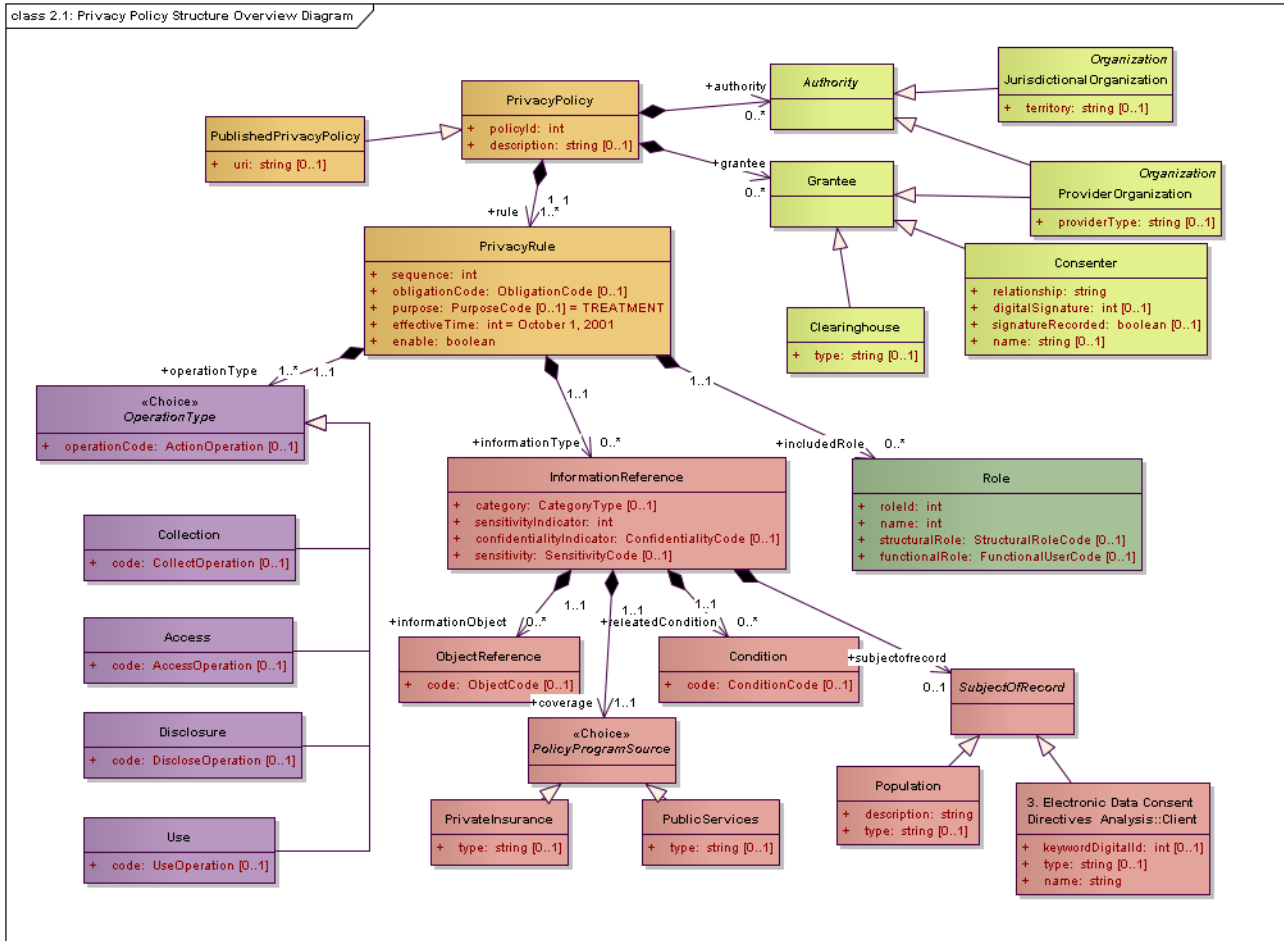


Illustration 6 Privacy Policy Information Model (Extracted from Composite Privacy Domain Analysis Model – DSTU – September 2009)

3.2.3 Consent Directive Information Model

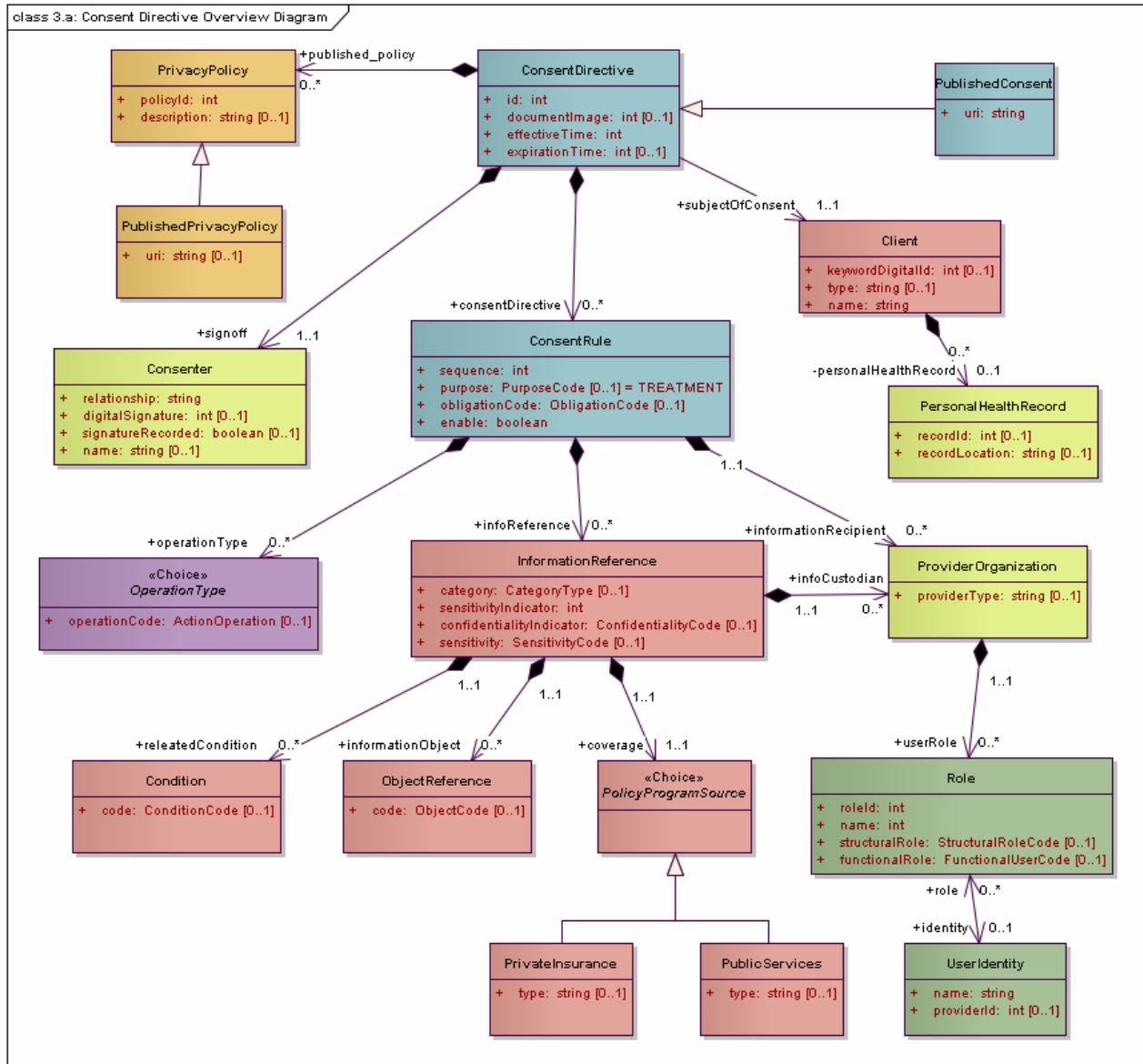


Illustration 7 Consent Directive Information Model (Extracted from Composite Privacy Domain Analysis Model – DSTU – September 2009)

3.3 Semantic Signifiers (Normative)

A semantic signifier is used to specify constraints on the information constructs that serve as payloads within service operations. It is the identification of a named set of information descriptions (e.g. semantic signifiers) that are supported by one or more operations. The reference points for associated conformance statements occur at the computational model interface where the semantic signifier is specified as an input or output required by the contract.

3.3.1 Access Request Message

Purpose

The Access Request Message encapsulates the information needed to request and enforce an access control decision.

The Access Request Message consists of three first-order business concepts: User, Resource, and Operation. User and Operation are identified in both Privacy and Security DAM's, while Target characteristics may be specified in policies, but a particular resource identifier will not be.

Attributes and assertions associated with a particular request message may be mapped to policy attributes as indicated (e.g. Purpose of Use, an attribute of Basic Policy is represented as a request attribute that is used as Access Decision Information).

The healthcare-specific semantic elements are identified in Illustration 11, below.

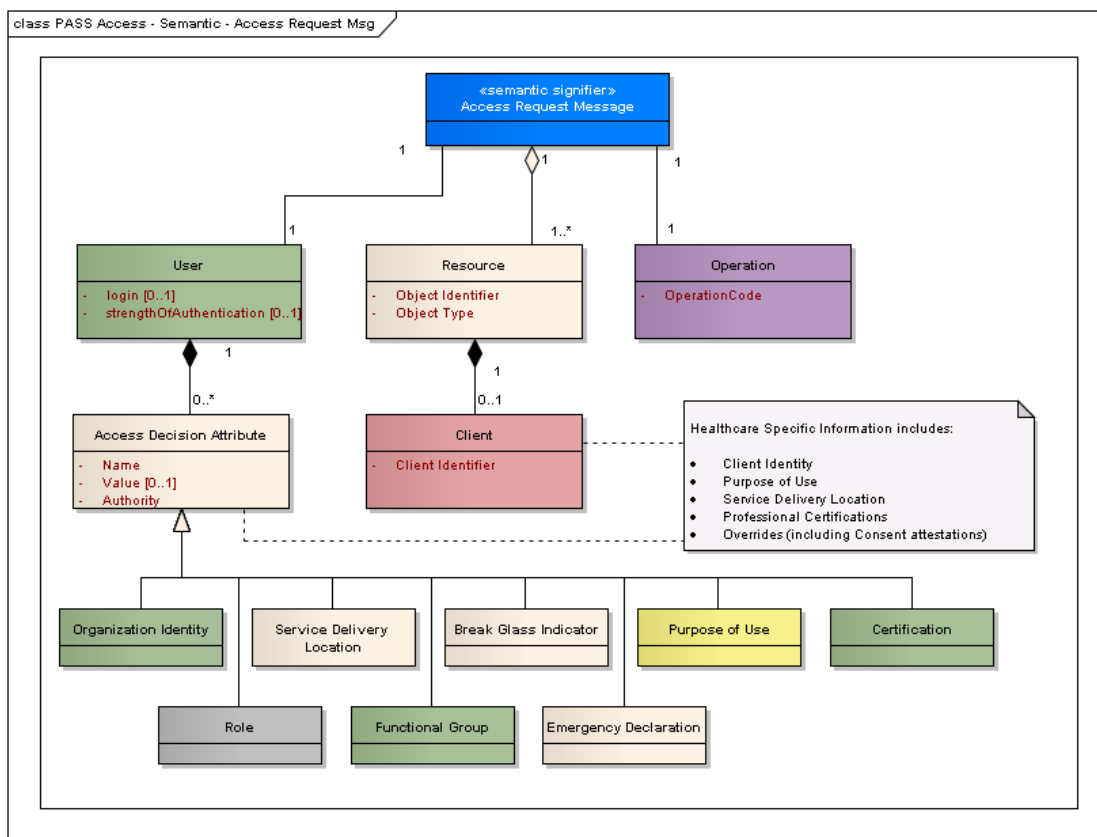


Illustration 8 Access Request Message

Details of the Access Request Message business concepts and attributes are as follows:

| Concept | Attribute | Description |
|---------|--------------------|--|
| User | Requestor Identity | A unique identifier associated with the User or Service Requestor. Some identity federation mechanism is |

| | | |
|-----------------------|-------------------------|--|
| User | Authentication Strength | assumed to enable mapping of requestor identities to User identities specified in any policy. A User may be a human or a machine actor. Mandatory. A coded concept indicating the strength of the authentication process used to identity the User. This attribute is associated directly with a Security Policy, however it is always in relation to the User making a specific request. Optional. |
| Assertion / Attribute | Name | The name (or type) associated with the assertion or attribute. |
| Assertion / Attribute | Value | The optional value of the attribute. Assertions general will not be associated with values. |
| Assertion / Attribute | Authority | The identity of the authority making the assertion or verifying the attribute. |
| Resource | Object Identifier | A unique identifier associated with the resource that is being accessed. |
| Resource | Object Type | The type of resource being requested. Object types are coded concepts from the HL7 V3 RBAC Constraint Catalogue. Optional. |
| Client | Client Identifier | A unique Client identifier, usually used to identify privacy policies or consent directives specific to that identifier. In order to support distributed policy stores, some federation mechanism will have to be implemented in order to assure identity correlation. Clients are associated only with the Resource being requested. Optional. |
| Operation | OperationCode | This is the coded concept from the HL7 V3 RBAC Constraint Catalogue. Mandatory. |

Assertions and attributes provide for flexibility and extensibility in the implementation of components that produce and consume the Access Request Message, however semantic interoperability requires that we specify the particular attributes that may be necessary for interoperability in the healthcare environment. Note that all of these attributes are optional, depending on the policy applicable to the request.

The table below details those attributes.

| Attribute | Description |
|---------------------------|--|
| Organization Identity | The unique identity associated with the organization that is responsible for the actions of the Requestor. |
| Service Delivery Location | The location from which the Requestor is providing service. |

| | |
|-----------------------|---|
| Break Glass Indicator | A coded concept which indicates the User-provided reason that the access control decision should be overridden. Policy will determine whether the User has the appropriate authority to make such as request and whether the request will be honored. |
| Purpose of Use | The specific purpose for the request. This might be assumed to be treatment/provision of care, may be determined by the Requestor's role in an RBAC access control environment, or specifically identified here. |
| Role | The structural role that the User is operating in for this request. |
| Functional Group | The functional role that the User is operating in for this request. |
| Emergency Declaration | An attestation from the User that they are operating in "Emergency Access" mode. |
| Certification | Any professional certification credentials that may be required for the request. Usually provided by a jurisdictional or professional body. |

3.3.2 Policy Selection Criteria

Purpose

Policy Selection Criteria consists of the semantics used to select one or more policies, specifically for the purpose of subsequent evaluation. In this context, there is a finite set of criteria that would be reasonable to use in order to facilitate the policy selection process.

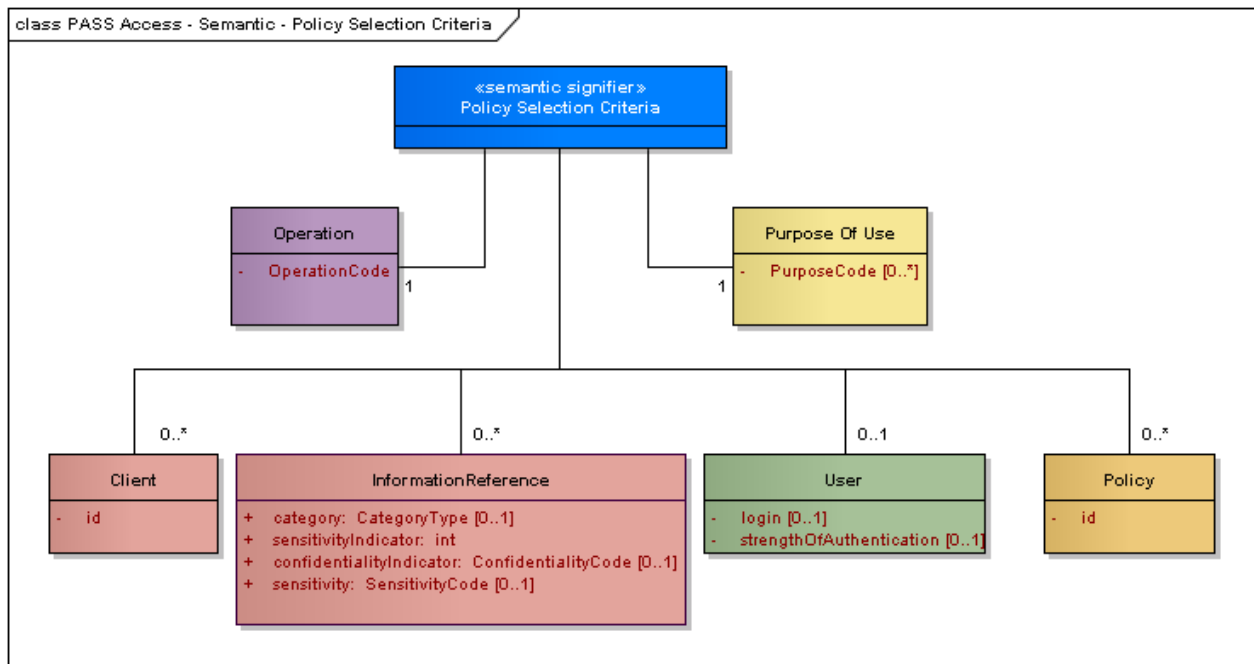


Illustration 9 Policy Selection Criteria

Details of the business concepts and attributes illustrated above are as follows:

| Concept | Attribute | Description |
|-----------------------|-------------------------|---|
| Operation | OperationCode | This is the coded concept from the HL7 V3 RBAC Constraint Catalogue. Mandatory. |
| Purpose Of Use | purposeCode | Purpose of Use identified for the collection, use, or disclosure of information. Mandatory. |
| Client | id | A unique Client identifier, usually used to identify privacy policies or consent directives specific to that identifier. In order to support distributed policy stores, some federation mechanism will have to be implemented in order to map identities. Optional. |
| Information Reference | category | Information category. |
| Information Reference | sensitivityIndicator | |
| Information Reference | confidentialiyIndicator | The confidentiality indicator is a coded attribute that assigns access controls on health records based on the information or type of access. ² Optional |
| Information Reference | sensitivity | Coded attribute that describes the sensitivity of a user or information artifact. ³ Optional. |
| Policy | id | The unique identifier of the policy being requested. The likely scenario where this would be populated is when a currently-executing policy references an external policy. Optional. |

3.3.3 Access Control Policy

Purpose

The Access Control Policy is the executable policy that is selected and evaluated to provide access control decisions. The Access Control Policy is described in the Security DAM (Informative) – January 2010 Ballot.

3.3.4 Attribute Selector (Informative)

Purpose

These name/value pairs are specific attributes associated with each of Client, Requestor, or Resource entities. A generic request/response semantic structure allows for a flexible and extensible set of attributes as shown in Illustration 7, below.

² Source: Security Domain Analysis Model – Draft

³ Source: Security Domain Analysis Model – Draft

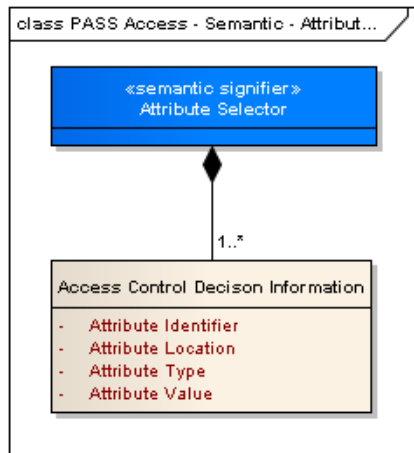


Illustration 10 Attribute Requisitioning and Provisioning

This semantic signifier will be constrained by the information models provided by the Composite Privacy DAM, and the Security DAM.

3.3.5 Privacy Policy and Consent Directive

Purpose

The Privacy Policy is the executable policy that is selected and evaluated to provide access control decisions in conjunction with Security Policies. A Consent Directives is a Client-specific instance of a Privacy Policy.

Privacy Policies and Consent Directives are described in the Composite Privacy DAM (DSTU) – September 2009 and can be referenced in the Information Viewpoint section of this document.

3.3.6 Access Control Decision (Informative)

Purpose

The Access Control Decision encapsulates the result of the access control request evaluation process, providing the decision along with any obligations that the applicable policy requires.

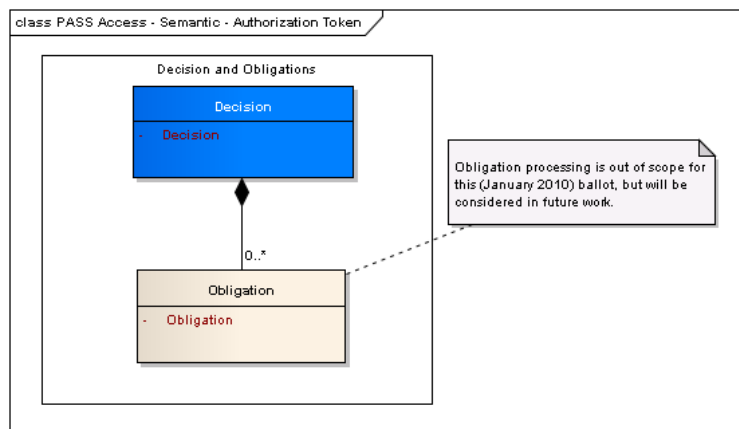


Illustration 11 Policy Decision and Obligations

Details of the business concepts and attributes illustrated above are as follows:

| Concept | Attribute | Description |
|------------|------------|--|
| Decision | Decision | A coded value indicating the decision that resulted from the evaluation of policy(ies) applicable to the request. |
| Obligation | Obligation | Coded value that describes technical or business obligations that are required to accompany the decision. Obligations are completely driven by policy. |

3.3.7 Policy Management Request

Purpose

The Policy Management Request encapsulates the lifecycle state transition events and associated information components for a Policy. Policy states are described in the Domain Analysis Models for both Composite Privacy (DSTU – September 2009), and Security (DSTU Ballot – January 2010).

In the illustration, Policy is shown as a generalization of both Privacy and Security policies as described in their respective DAMs. Please refer to those DAMs for detailed semantic information.

The following table describes the concepts and attributes from Illustration 10, below.

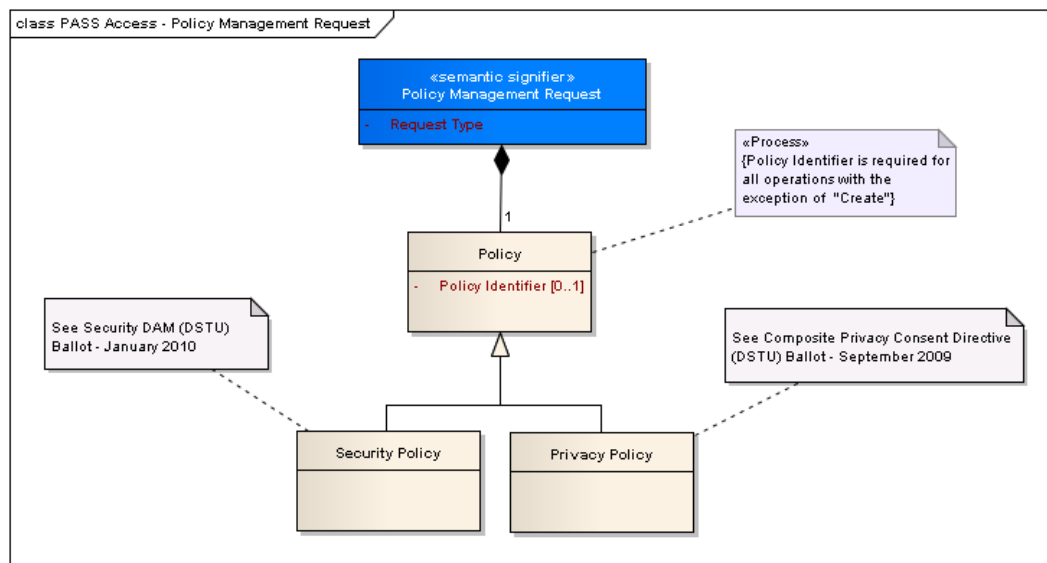


Illustration 12 Policy Management Request

| Concept | Attribute | Description |
|---------------------------|-------------------|--|
| Policy Management Request | Request Type | A coded value indicating the operation that is to be performed on the accompanying policy. Mandatory. |
| Policy | Policy Identifier | A unique identifier for the policy. Mandatory except when the request type indicates that a new policy is to be created. |

3.3.8 Policy Management Response

Purpose

The Policy Management Response encapsulates the results of an associated request for a lifecycle change a Policy. Policy states are described in the Domain Analysis Models for both Composite Privacy (DSTU – September 2009), and Security (DSTU Ballot – January 2010).

The following table describes the concepts and attributes from Illustration 12, below.

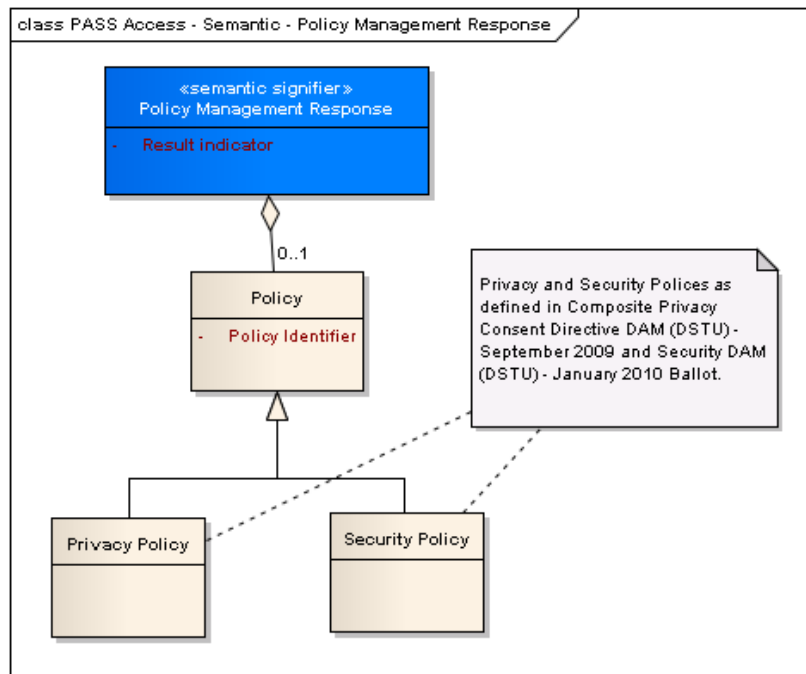


Illustration 13 Policy Management Response

| Concept | Attribute | Description |
|----------------------------|-------------------|---|
| Policy Management Response | Result Indicator | A coded value indicating the result of the operation that was requested. Mandatory. |
| Policy | Policy Identifier | A unique identifier for the policy. Mandatory when Policy is present. |

3.4 Dynamic Model

The conceptual lifecycle illustrated below allows a policy to be managed from inception, through to obsolescence.

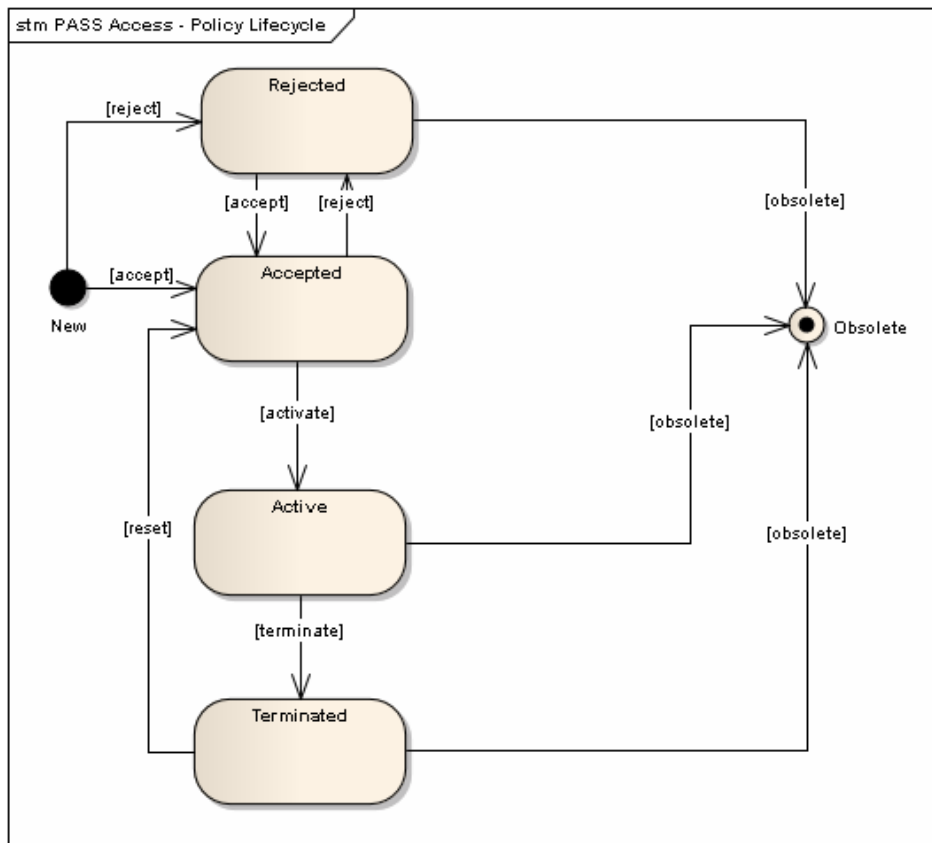


Illustration 14 Policy Conceptual Lifecycle

A policy starts as a new item. A security or privacy domain can accept the policy or reject it. This allows for manual or automated review processes to occur prior to activation.

If a policy is rejected, it can be subsequently accepted (e.g. on an appeal) or it can be declared obsolete.

Accepted Policies may be activated or rejected. Activation may be a manual process, or can be automated, for example as a result of the policy’s effective date being reached.

Once activated, the expectation is that the policy has been agreed to by the domain. The expectation is that this would be the only state in which the policy would be used to make access control decisions upon.

An active policy can be made immediately and irrevocably obsolete, or it can be terminated.

Terminated policies can be reset to enter the lifecycle or made obsolete.

4 Computational Viewpoint

4.1 Overview

A computational viewpoint on an SAEAF/RM-ODP system and its environment is a specification that enables distribution of the functional behavior of the system into service components which interact at interfaces. In the computational viewpoint, applications and business process realizations consist of configurations of interacting service components reflecting business roles participating in service collaborations.

4.2 Capabilities

This section describes each of the behaviors that have been identified from the requirements. The attributes of Accountability Type, Role, and Dependencies act to provide input to determining what collaborations may be required to ensure that any contract associated with the capability is fulfilled.

4.2.1 Enforce Access Control Decision

| | |
|--|--|
| Name | Enforce Access Control Decision |
| Description | Accepts a request to access a resource and invokes Policy Decision Points to provide decisions and obligations. Based upon those decisions the service allows or prevents the request to be fulfilled. |
| Accountability Type | Authorization |
| Role | Policy Enforcement Point (Access Enforcement Function) |
| Obligations | To enforce access control decisions made by Policy Decision Points by allowing or refusing requests to access protected resources. |
| Community | Indirectly, all Protected Resources |
| Prohibitions | |
| Dependencies | Request Access Control Decision Submit Audit Record |
| Precondition | |
| Constraints | |
| Postconditions | The requested resource has been made available to the requestor. |
| Exception Conditions | Requestor does not have the authority to access the requested resource for the . |
| Relationship to levels of conformance | |

4.2.2 Request Access Control Decision

| | |
|--|---|
| Name | Request Access Control Decision |
| Description | Accepts a request to access a protected resource and provides a permit/deny decision |
| Accountability Type | Authorization |
| Role | Policy Decision Point (Access Decision Function) |
| Obligations | To evaluate access control policies applicable to the request and render a decision. |
| Community | Used by Policy Enforcement Points |
| Prohibitions | |
| Dependencies | Provide Access Decision Information Process Access Control Policy |
| Preconditions | |
| Constraints | |
| Postconditions | An access control decision and any applicable obligations have been provided to the requestor based upon the evaluation of one or more applicable policies. |
| Exception Conditions | No applicable policy exists to base a decision on. Requestor does not have the authority to invoke the capability. |
| Relationship to levels of conformance | |

4.2.3 Get Access Decision Information

| | |
|--|--|
| Name | Get Access Decision Information |
| Description | Accepts a request to return access control decision attributes. |
| Accountability Type | Attribute |
| Role | Policy Information Point |
| Obligations | To provide access control decision information that matches the incoming criteria. |
| Community | Used by Policy Decision Point |
| Prohibitions | |
| Dependencies | <<External>> Client Attributes <<External>> Resource Attributes <<External>> User Attributes <<External>> Environment Attributes |
| Preconditions | |
| Constraints | |
| Postconditions | The requested attribute values has been returned |
| Exception Conditions | One or more attribute identifiers are unknown. One or more attribute values are unavailable. Requestor does not have the authority to invoke the capability. |
| Relationship to levels of conformance | |

4.2.4 Get Policy

| | |
|--|--|
| Name | Get Policy |
| Description | Accepts a request to return any policies that match the incoming criteria. |
| Accountability Type | Policy |
| Role | Policy Provider |
| Obligations | To provide access control policies matching the incoming criteria. |
| Community | Used by Policy Decision Point |
| Prohibitions | |
| Dependencies | <<External>> Policy Administration |
| Preconditions | |
| Constraints | |
| Postconditions | Zero or more machine-readable policies have been returned to the requestor. |
| Exception Conditions | The requestor does not have the authority to enable the request to be processed. |
| Relationship to levels of conformance | |

4.2.5 Submit Access Control Policy

| | |
|---|---|
| Name | Submit Access Control Policy |
| Description | Accepts a request to integrate a policy into an existing policy store. |
| Accountability Type | Policy |
| Role | Policy Store |
| Obligations | To receive privacy and/or security policies. |
| Community | Used by Policy Management |
| Prohibitions | |
| Dependencies | <<External>> Policy Management |
| Preconditions | |
| Constraints | |
| Inputs | Access Request Message Access Control Policy |
| Outputs | None identified. |
| Postconditions | Zero or more machine-readable policies have been processed. |
| Exception Conditions | The requestor does not have the authority to enable the request to be processed. |
| Relationship to levels of conformance | |
| Miscellaneous notes | |
| Healthcare-specific requirements satisfied | AC12 – Support healthcare-specific security and privacy constraints on access control rules AC43 – Incorporate standard healthcare-specific access control information code sets per HL7 security and privacy domain information models. |

4.2.6 Submit Audit Record⁴

| | |
|--|---|
| Name | Submit Audit Record |
| Description | Submits an appropriately-formatted audit record. See PASS-Audit Functional Model for details. |
| Accountability Type | Audit |
| Role | Audit Event Source |
| Obligations | Provide audit event information |
| Community | Audit Event Sink |
| Prohibitions | |
| Dependencies | PASS-Audit - Submit Audit Record capability |
| Precondition | The audit service has been instantiated and the submitting service configured to invoke it. |
| Constraints | |
| Postconditions | An audit event record has been received by the Audit Event Sink. |
| Exception Conditions | |
| Relationship to levels of conformance | |

⁴ The capability and its associated semantic content will be defined in a forthcoming PASS-Audit Conceptual Model.

4.2.7 Manage Policy

| | |
|--|---|
| Name | Manage Policy |
| Description | Accepts a request manage a Privacy or Security Policy. "Manage" includes create, update, and delete operations. |
| Accountability Type | Policy |
| Role | Policy Manager |
| Obligations | To manage the lifecycle of privacy and security policies. |
| Community | Policy Managers, Policy provisioning actors |
| Prohibitions | |
| Dependencies | Audit |
| Preconditions | |
| Constraints | |
| Postconditions | A machine-readable policy lifecycle has been altered. |
| Exception Conditions | The requestor does not have the authority to enable the request to be processed. |
| Relationship to levels of conformance | |

4.3 Collaboration Analysis

This section discusses the interactions between capabilities classified by roles⁵. It also identifies the obligations associated with those roles as well as the interdependencies of the capabilities.

4.3.1 Access Control

Illustration 15 Access Control Roles and Capabilities, on the following page shows a static representation of the relationships between various roles participating in the execution of “Enforce Access Control Decision” behavior and associates capabilities with accountabilities in order to provide additional basis for profile development.

The roles named in the illustration correspond to those identified in the Business Viewpoint (Authorization Reference Model) in order to ensure consistency and traceability between artifacts.

The following conventions have been used to create the diagram:

- Each role is identified as a particular collection of related capabilities.
- The stereotype for each port identifies the accountability type for its associated behavior.
- The dependency arrows point to the provider of the capability.
- Binding semantics are identified on the dependency connectors and the associated arrows indicate the source and destination of each of those information components.

Note that the illustration shows an Access Control Intercept, with an embedded Policy Enforcement Point. This is consistent with the representation of Access Control functions contained in ISO/IEC 10181-3.

⁵ The term “role” is overloaded when dealing with an architecture framework and security concepts in the same document. In an effort to increase clarity, the use of term “role” on its own denotes identification for behavior that reveals a capability, capacity, or competency from an architectural perspective. When referring to “roles” associated with privacy and security, the terms “functional role” and “structural role” will be used.

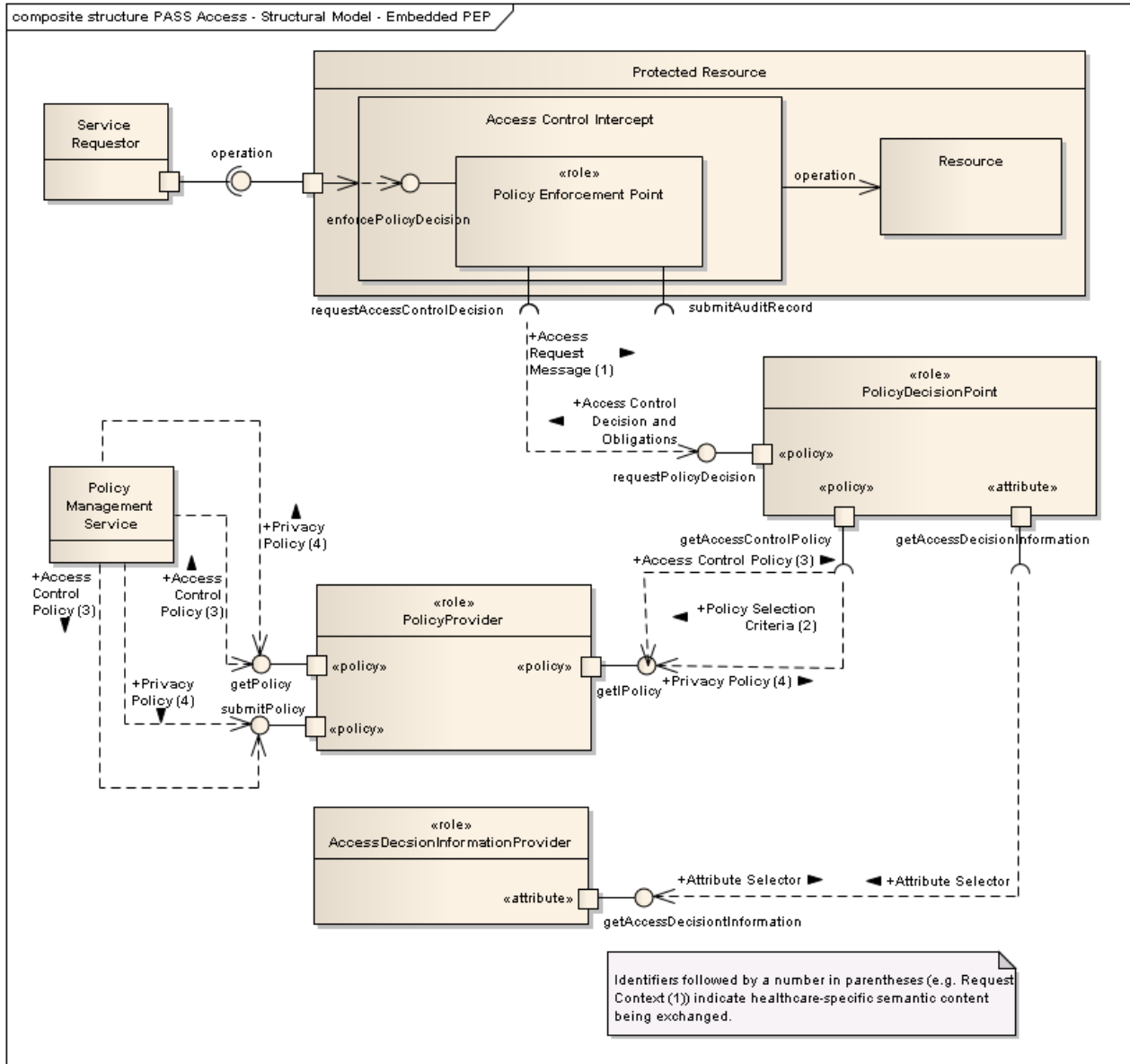


Illustration 15 Access Control Roles and Capabilities

A sequence diagram follows which illustrates the collaborations necessary to complete the “Enforce Policy Decision” capability. Note that the lifelines or objects identified represent business roles rather than specific components.

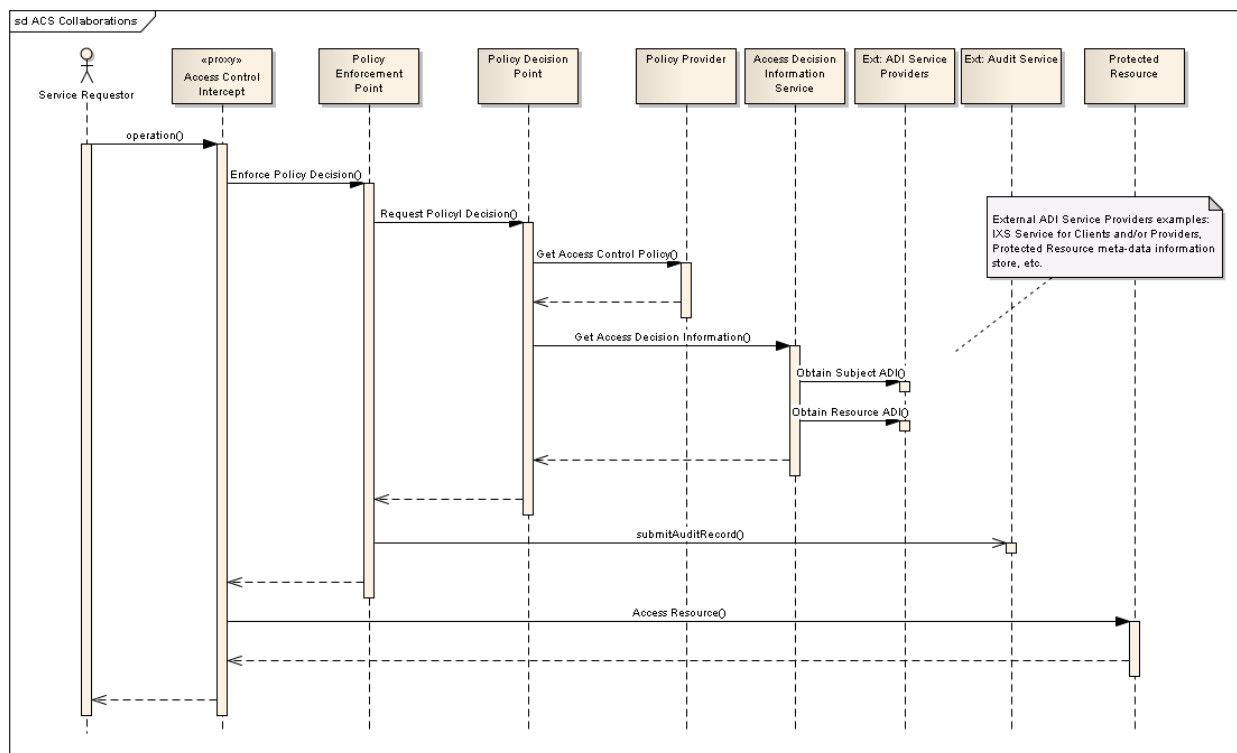


Illustration 16 Capability Collaborations for Enforce Policy Decision

1. A Service Requestor makes a request for a Protected Resource and includes the Requestor's identity and credentials. The request is intercepted by an Access Control component acting as a proxy for the Resource.
2. The Access Control Intercept requests that an internal Policy Enforcement Point (PEP) enforce an access control decision and provides an authorization request to the PEP. The authorization request includes the Access Request Message consisting of Requestor identity and credentials, the Resource identifier(s), and the operation requested.
3. The PEP requires Request Policy Decision and Submit Audit Record capabilities to be supplied in order to fulfill its role. This set of capabilities is exposed by the business roles of Policy Decision Point (PDP) and External Audit Service, respectively. The PEP requests a policy decision to be made by the PDP. The PDP is provided with Access Request Message that the PEP received, augmented with any additional contextual information that the PEP can provide.
4. The PDP must have a policy to evaluate and assuming that no applicable policy is available internally, invokes Get Access Control Policy behavior from a Policy Provider, providing a set of policy selection criteria for the Policy Provider to determine which policy(ies) to return.
5. During the evaluation of the Policy, the PDP requires additional information (i.e. information that is referred to in the policy, but not contained in the Access Request Message provided). The PDP invokes the Get Access Decision Information on an Access Decision Information Service.

6. The Access Decision Information Service invokes a set of behaviors on external services to obtain additional Requestor, Client, Resource, and Environment ADI that may be associated with the request.
7. Once the ADI has been obtained, the PDP can evaluate the applicable policy and render a decision. Depending upon the policy semantics, the decision may be contingent on one or more obligations that will be returned to the PEP to enforce.
8. As a result of this service invocation, the PEP has an obligation to generate audit event information, and ultimately to provide that audit information to a component acting as an Audit Service for the PEP.

4.3.2 Policy Management

The Policy Manager role fulfills the capabilities associated with the lifecycle and provisioning of executable privacy and security policies. Policy classes that inform attributes of privacy and security policies are contained in the Composite Privacy DAM (DSTU) – Sept 2009, and Security DAM – January 2010 (Informative Ballot).

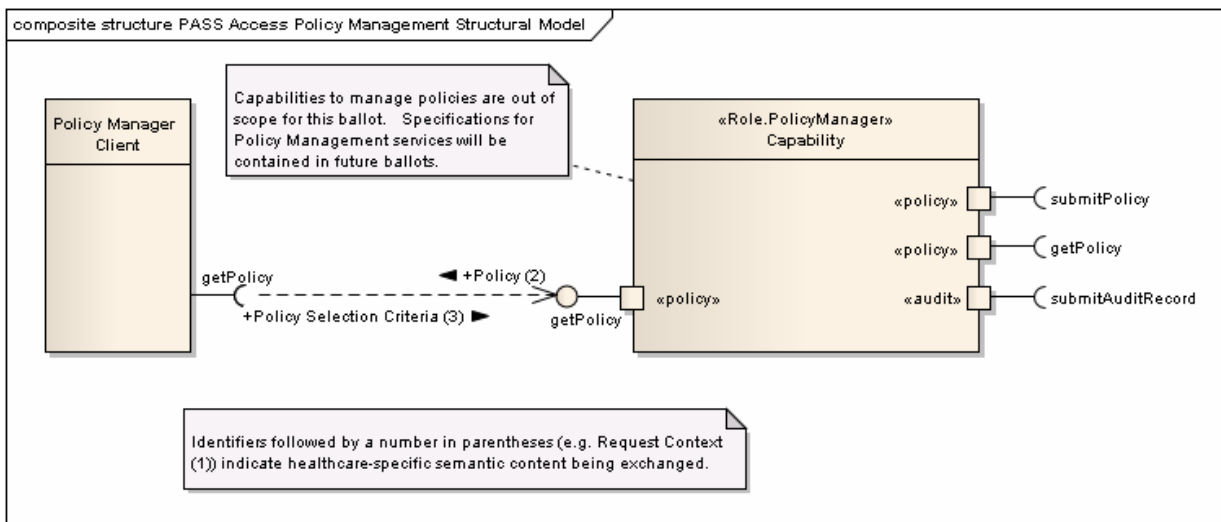


Illustration 17 Policy Management Roles and Capabilities

4.4 Conformance (Normative)

This section identifies those contracts and profiles that will be necessary for working interoperability.

In the computational viewpoint, there exists a reference point at any interface of any service component. A conformance statement is a statement that identifies conformance points of a specification and the behavior which must be satisfied at these points. Each reference point can become a conformance point based on conformance assertions made by referencing specifications in other viewpoints or less abstract specifications at a platform independent or platform specific level.

A contract can apply at a given reference point in a system. Conformance relies on evaluating the interactions between roles against their contractual obligations. In that case, it specifies the functional behavior which can be expected at the reference point.

Conceptual-level conformance statements will only occur in standards which are intended to constrain some feature of a real implementation, so that there exists, in principle, the possibility of testing. The following contract specifications and conformance profiles constitute conceptual conformance statements.

Note: At this point, healthcare-specificity stems from the combination of cross-industry access control standards with healthcare-specific semantics.

4.4.1 Contracts

Contracts tie capabilities to the semantic content required to execute the behavior associated with those capabilities.

The tables below identify the specific healthcare requirements that are satisfied by the contract. The rows entitled Inputs and Outputs identify the specific Semantic Signifiers that are bound to the capability to make the contract normative.

Access Control

| | |
|---|--|
| Capability Name | Enforce Access Control Decision |
| Description | Accepts a request to access a resource and invokes Policy Decision Points to provide decisions and obligations. Based upon those decisions the service allows or prevents the request to be fulfilled. |
| Inputs | Access Request Message |
| Outputs | Authorization token – an indicator that the Access Control Service has permitted or denied the request. |
| Miscellaneous notes | Invokes “ Request Access Control Decision ” from access decision functions or Policy Decision Points. |
| Healthcare-specific Requirements satisfied | <p>ACG-1 – Provide healthcare authorization and access control as a service.</p> <p>ACG-2 – Provide the capability to ensure that protected information is accessible only by entities possessing authorizations that meet or exceed healthcare information security and privacy policy access control decision attributes.</p> <p>ACG-4 – Incorporate standard healthcare-specific access control information code sets per HL7 security and privacy domain models.</p> |

Access Control Decision

| | |
|---|--|
| Capability Name | Request Access Control Decision |
| Description | Accepts a request to access a protected resource and provides a permit/deny decision |
| Inputs | Access Request Message |
| Outputs | Access Control Decision |
| Healthcare-specific Requirements satisfied | <p>ACG-4 – Incorporate standard healthcare-specific access control information code sets per HL7 security and privacy domain models.</p> <p>AC1-2 - Request access control decision information (ADI, i.e.: policy attribute values) from another service.</p> <p>AC1-3 - Provide the capability to return both a response and its associated obligation policy following a request for information.</p> <p>AC2-7 - Request a machine-readable policy document from another service.</p> |

Resolve ADI Request

| | |
|---|--|
| Capability Name | Get Access Decision Information |
| Description | Accepts a request to return access control decision attributes. |
| Inputs | Attribute Selector |
| Outputs | Attribute Selector |
| Miscellaneous notes | |
| Healthcare-specific Requirements satisfied | <p>AC1-1 – Provide access control decision information (ADI, ie: policy attribute values) to another service.</p> <p>AC2-7 - Request a machine-readable policy document from another service..</p> <p>AC1-2 – Request access control decision information (ADI, i.e.: policy attribute values) from another service.</p> |

Query Policy

| | |
|---|--|
| Capability Name | Get Policy |
| Description | Accepts a request to return any policies that match the incoming criteria. |
| Inputs | Policy Selection Criteria |
| Outputs | Access Control Policy |
| Postconditions | Zero or more machine-readable policies have been returned to the requestor. |
| Exception Conditions | The requestor does not have the authority to enable the request to be processed. |
| Relationship to levels of conformance | Informative |
| Miscellaneous notes | A required interface where policies need to be “pulled in” prior to execution, or where policy attributes need to be determined. |
| Healthcare-specific Requirements satisfied | AC2-8 – Receive a request for a machine-readable policy document from another service. |

Accept Policy

| | |
|------------------------|---|
| Capability Name | Submit Access Control Policy |
| Description | Accepts a request to integrate a policy into an existing policy store. |
| Inputs | Access Request Message Access Control Policy |
| Outputs | None identified. |

| | |
|---|---|
| Postconditions | Zero or more machine-readable policies have been processed. |
| Exception Conditions | The requestor does not have the authority to enable the request to be processed. |
| Relationship to levels of conformance | |
| Miscellaneous notes | |
| Healthcare-specific requirements satisfied | AC2-9 – Support exchange of security and privacy policy documents with other access control service. ACG-4 – Incorporate standard healthcare-specific access control information code sets per HL7 security and privacy domain models. |

Manage Policy

| | |
|---|---|
| Capability Name | Manage Policy |
| Description | Accepts a request manage to a Privacy or Security Policy. “Manage” includes create, update, and delete operations. |
| Inputs | Policy Management Request |
| Outputs | Policy Management Response |
| Miscellaneous notes | Informative |
| Healthcare-specific requirements satisfied | AC09 – Support any combination of healthcare-specific role, context, or entity-based policies. AC12 – Support healthcare-specific security and privacy constraints on access control rules AC43 – Incorporate standard healthcare-specific access control information code sets per HL7 security and privacy domain information models. |

Submit Audit Information

| | |
|---|--|
| Capability Name | Submit Audit Record |
| Description | Accepts a request manage to a Privacy or Security Policy. “Manage” includes create, update, and delete operations. |
| Inputs | Audit record conformant to PASS Audit specification |
| Outputs | None |
| Miscellaneous notes | Informative – The semantic signifiers for this contract will be described in a future PASS Audit ballot. |
| Healthcare-specific requirements satisfied | ACG-3 – Generate security audit records based on healthcare-specific security relevant events. |

4.4.2 Conformance Profiles

A Conformance Profile in the context of this document consists of a set of contracts which, taken together, provide complete, coherent behavior against which conformance can be claimed at both Platform Independent, and Platform Dependent levels of specificity. Conformance profiles at this level provide the foundation for working operability. These profiles may optionally include additional constraints where relevant.

Access Control Service 1 (ACS1)

The ACS1 profile consists of the contracts that are consistent with the ISO and OASIS concepts of an enforcement function/point, which relies on separate behavior for policy evaluation

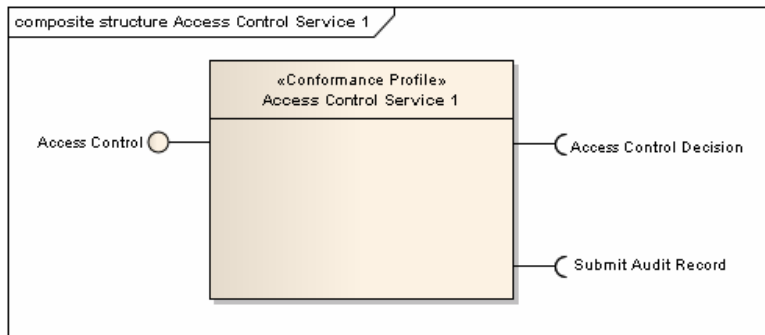


Illustration 18 - Conformance Profile: Access Control Service 1

Contracts: Access Control
 Access Control Decision
 Submit Audit Record

Access Control Decision 1 (ACD1)

The ACD1 profile consists of those contracts necessary to provide a policy decision and retrieve and accept policies from an external policy store. The profile relies on external services to provide ADI.

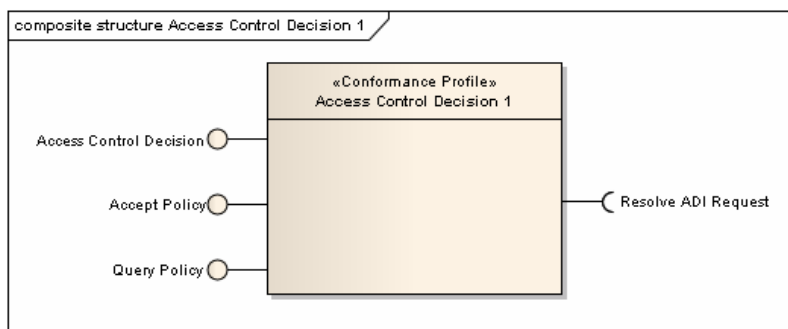


Illustration 19 - Conformance Profile: Access Control Decision 1

Contracts: Access Control Decision
 Resolve ADI Request

Accept Policy
Query Policy

Access Control Decision 2 (ACD2)

This profile provides Access Control Decisions, but does not support policies provisioned from external sources.

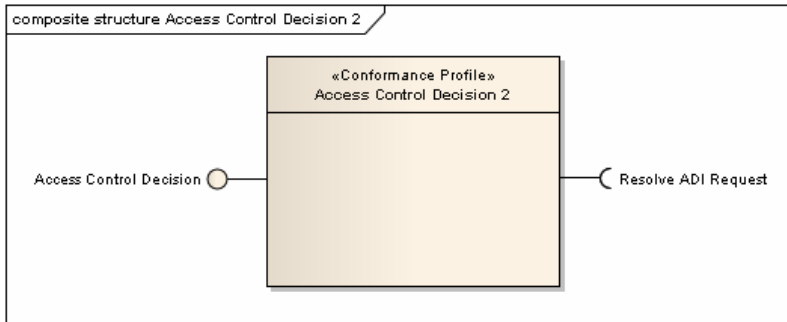


Illustration 20- Conformance Profile: Access Control Decision 2

Contracts: Access Control Decision
 Resolve ADI Request

ADI Provisioner

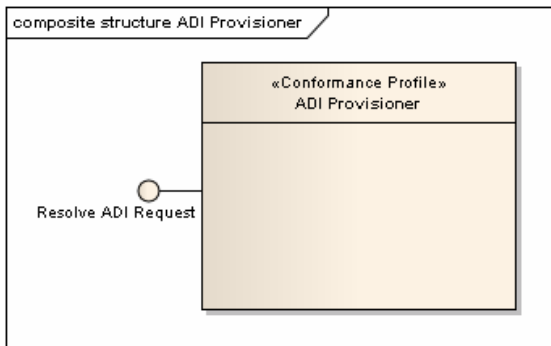


Illustration 21 - Conformance Profile: ADI Provisioner

Contracts: Resolve ADI Request

AC Policy Provisioner

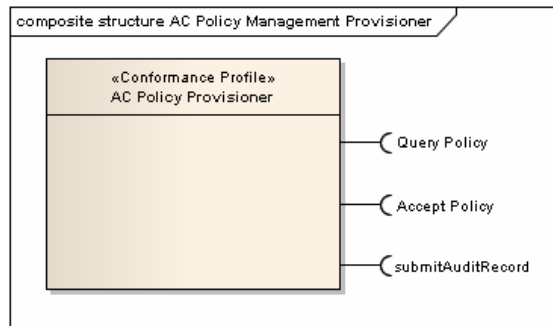


Illustration 22 - Conformance Profile: AC Policy Provisioner

Contracts: Query Policy
 Accept Policy

5 Engineering Viewpoint

This section identifies the infrastructure that is required to support functional distribution of an ODP system⁶ at the conceptual level.

5.1 ODP Functions

The ODP Functions are specified by the Reference Model and are intended to provide broad categories of functions to be considered. At the conceptual level, the majority of these functions would not necessarily be filled.

5.1.1 Physical Distribution Functions

N/A

5.1.2 Communication Functions

The communication functions involved in the distribution of healthcare-specific information mustN/A

5.1.3 Processing Functions

N/A

5.1.4 Storage Functions

N/A

5.2 Engineering Roles

None identified.

⁶ ISO/IEC 10746-3 Open Distributed Processing – Reference Model Architecture

6 Appendix A - Glossary of Terms

The following table identifies terms used in this document that are specific to the subject domain.

| Term | Definition | Source |
|--|---|--|
| Access Control | A means of ensuring that the resources of a data processing system can be accessed only by authorized entities in authorized ways | ISO/IEC 2382-8, definition 08.04.01 |
| Access Control Information (ACI) | Any information used for access control purposes, including contextual information. Contextual information might include source IP address, encryption strength, the type of operation being requested, time of day, etc. Portions of ACI may be specific to the request itself, others may be associated with the connection via which the request is transmitted, others (e.g., time of day) may be "environmental". | ISO TS 22600-1: 2006 OASIS |
| Attribute Directory | A source of attribute data items | |
| Audit record | Data structure used to record audit events | |
| Authorization | A process of granting rights, which includes the granting of access rights | ISO TS 22600-1: 2006 |
| Authorization/attribute access control | Access control based on values of access control information | |
| Behavior | The manner in which activity is exhibited | |
| Break glass | An administrative control which allows an authorized individual to access information under specific, declared circumstances. | |
| Business context | Enterprise requirements | |
| Compatible | Non contradictory (not necessarily identical) | |
| Composable | Capable of being combined with other like components to form a new capability | |
| Consent, patient | Permission granted, withdrawn, or withheld by an individual, usually for the collection, access, use, or disclosure of personal information or individually identifiable health information for a given purpose. | |
| Consistent time | A mechanism to synchronize the time base between multiple actors and computers. | IHE IT Infrastructure Technical Framework, Vol 1, Rev. 6.0 |
| Constraint (authorization) | A limitation on an access control rule | |
| Decision, access control | Finite result of evaluating an access control policy for a given set of Access Control Information | |
| Decision, policy | See Decision, access control | |
| Dependency | Requirement to consult another entity | |
| Directive, patient consent | An instruction regarding consent to collect, use, and/or disclose Individually Identifiable Health Information | |

| Term | Definition | Source |
|--|--|---------------------|
| Discovery | Act of seeking and finding a target | |
| Document, clinical | Documentation of clinical observations and services | |
| Domain | A collection of resource consumers, information and functional resources, and the policy that binds them. | |
| Emergency access | Access permitted by policy when an emergency condition exists | |
| Environment | Surrounding space | |
| Environmental variables | Those aspects of policy required for an authorization decision that are not contained within static structures, but are available through some local means to a privilege verifier (e.g. time of day, or current account balance). | ISO TS 22600-3:2006 |
| Event | Occurrence of a condition | |
| Event, security relevant | Event that is included in security policy | |
| Capability, functional | Capacity to exhibit a relevant behavior | |
| Granularity | Level of detail | |
| Individually Identifiable Health Information | Health Information that contains or can be reconstituted to refer to an specific, identifiable individual. | |
| Integration | The act of bringing together data and/or capabilities from two or more independent applications, within the same enterprise or across multiple enterprises | |
| Interaction | Participation in joint activity | |
| Interface | Point where interchange of data takes place | |
| Interoperability | Ability to coordinate operations in a meaningful way | |
| Machine readable | Capable of being processed by a computer in a meaningful way | |
| Maintenance | Administration to ensure acceptable operation | |
| Management services | Functions needed to conduct establishment, review, and maintenance | |
| Object | Any system resource subject to access control, such as a file, printer, terminal, database record | |
| Obligation/promise | Constraint dealing with required behavior | |
| Permission | An operation on an object [INCITS 359-2004] | |
| Policy | A set of legal, political, organizational, functional and technical obligations for communication and cooperation | ISO TS 22600-1:2006 |
| Policy Decision Point (PDP) | A system entity that makes authorization decisions for itself or for other system entities that request such decisions. | OASIS |
| Policy Enforcement Point (PEP) | A system entity that requests and subsequently enforces authorization decisions. | OASIS |
| Policy Information Point (PIP) | The system entity that acts as a source of <i>attribute</i> values. | OASIS |
| Policy Administration Point (PAP) | The system entity that creates a <i>policy</i> or <i>policy set</i> . | OASIS |

| Term | Definition | Source |
|-----------------------------|--|--------|
| | | |
| Policy administration | Management of policy rules | |
| Policy, nested | Policy rules stated in a hierarchical fashion | |
| Profile | A named set of cohesive capabilities | |
| Profile, conformance | Profile that specifies compliance with a specification | |
| Profile, functional | Named list of a subset of the operations defined within this specification which must be supported in order to claim conformance to the profile. | |
| Provisioning | Supplying of items to a membership class | |
| Purpose of use | Stated intent for access to privacy data | |
| Repository, directive | Source of policy directives | |
| Repository, policy | Source of policy rules | |
| Role, functional | Named set of permissions controlling fine-grained accesses within a resource such as an application | |
| Role, structural | Named set of permissions controlling coarse-grained access at the outer boundary of a resource such as an application | |
| Rule-based access control | Access control based on evaluation of a set of rules | |
| Scalable | Ability to be successfully applied to a range of sizes and/or complexities | |
| Schema | Format specification with meaningful components | |
| Security logic | Software specification of security actions and conditions | |
| Security policy enforcement | Security policy enforcement deals with ensuring that users attempting to access system functions and data possess attributes (such as privileges granted and provisioned in security and privacy management) equal to or greater than that required for the access | |
| Service consumer | A component that uses a service | |
| Service provider | A component that provides a service | |
| Subject | Person to whom data pertains | |
| Synchronization, policy | Mutual modification of policy to achieve compatibility | |
| Targeted | Selected for communication | |
| Vocabulary | Language terms pertaining to a domain of discourse | |

7 Appendix B - Related Standards

The following standards are referenced and provide foundational components for this work:

- ISO/IEC 10181-3:1996 – Information Technology – Open Systems Interconnection – Security Frameworks for Open Systems: Access Control Framework – Access Enforcement Function “intercept” modeling
- ISO 22600 series – Policy Management and Access Control – Basic Access Control Model
- OASIS XACML 2.0 Specification – Terminology