5.5.1 - Access Control Policies

Contents of this Page

- Summary
  - Description of the profile
  - Capabilities
- Requirements traceability
- accessContolPolicyModel
  - Description
  - Requirements addressed
  - Overview of possible operations
- assembly
  - Description
  - Requirements addressed
  - Overview of possible operations
- binding
  - Description
  - Requirements addressed
  - Overview of possible operations
- complianceDiscovery
  - Description
  - Requirements addressed
  - Overview of possible operations
- componentAcquisition
  - Description
  - Requirements addressed
  - Overview of possible operations
- compositionArchive
  - Description
  - Requirements addressed
  - Overview of possible operations
- compositionChange
  - Description
  - Requirements addressed
  - Overview of possible operations
- configurationManagement
  - Description
  - Requirements addressed
  - Overview of possible operations
- discovery
  - Description
  - Requirements addressed
  - Overview of possible operations
- identity
  - Description
  - Requirements addressed
  - Overview of possible operations
- interactionLog
  - Description
  - Requirements addressed
  - Overview of possible operations
- interactionResults
  - Description
  - Requirements addressed
  - Overview of possible operations
- interoperabilityDiscovery
  - Description
  - Requirements addressed
  - Overview of possible operations
- logging
  - Description
  - Requirements addressed
  - Overview of possible operations
- mediation
  - Description
  - Requirements addressed
  - Overview of possible operations
- metadata
  - Description
  - Requirements addressed
  - Overview of possible operations
• metrics
  ◦ Description
  ◦ Requirements addressed
  ◦ Overview of possible operations
• metricsDiscovery
  ◦ Description
  ◦ Requirements addressed
  ◦ Overview of possible operations
• monitor
  ◦ Description
  ◦ Requirements addressed
  ◦ Overview of possible operations
• monitoring
  ◦ Description
  ◦ Requirements addressed
  ◦ Overview of possible operations
• policyAdministration
  ◦ Description
  ◦ Requirements addressed
  ◦ Overview of possible operations
• policyAlternative
  ◦ Description
  ◦ Requirements addressed
  ◦ Overview of possible operations
• policyAssertion
  ◦ Description
  ◦ Requirements addressed
  ◦ Overview of possible operations
• policyAudit
  ◦ Description
  ◦ Requirements addressed
  ◦ Overview of possible operations
• policyAuthorityDelegation
  ◦ Description
  ◦ Requirements addressed
  ◦ Overview of possible operations
• policyComposition
  ◦ Description
  ◦ Requirements addressed
  ◦ Overview of possible operations
• policyConflictResolution
  ◦ Description
  ◦ Requirements addressed
  ◦ Overview of possible operations
• policyConstraint
  ◦ Description
  ◦ Requirements addressed
  ◦ Overview of possible operations
• policyDecision
  ◦ Description
  ◦ Requirements addressed
  ◦ Overview of possible operations
• policyDecisionProcedures
  ◦ Description
  ◦ Requirements addressed
  ◦ Overview of possible operations
• policyDistribution
  ◦ Description
  ◦ Requirements addressed
  ◦ Overview of possible operations
• policyEnforcement
  ◦ Description
  ◦ Requirements addressed
  ◦ Overview of possible operations
• policyMetrics
  ◦ Description
  ◦ Requirements addressed
  ◦ Overview of possible operations
• policyObligation
  ◦ Description
  ◦ Requirements addressed
  ◦ Overview of possible operations
• policyRefinement
  ◦ Description
  ◦ Requirements addressed
  ◦ Overview of possible operations
Summary

Description of the profile

Service policies help establish constraints on the service specifications and mandate an approach. Policies can be specified around access control constraints.

Access Control Policies include the following capabilities:

- creation, deletion, edit, maintenance of access control policy models

Access Control Policies are a kind of Policy and Contract and consequently specialize capabilities architecturally implied by the concept of Policy and Contract.

Providing SOA security in an ecosystem of governed services has the following architectural implications on the policy support and the distributed nature of mechanisms used to assure SOA security:

- Security policies require mechanisms to support security description administration, storage, and distribution.
- Service descriptions supporting security policies should: have a meta-structure sufficiently rich to support security policies; be able to reference one or more security policy artifacts; have a framework for resolving conflicts between security policies.

It is assumed that the platform implementation:

- provides protection of the confidentiality and integrity of message exchanges;
- is distributed so as to provide centralized or decentralized policy-based identification, authentication, and authorization;
- is able to scale to support security for a growing ecosystem of services;
- is able to support security between different communication technologies;

It is assumed that platform security services include:

- services that abstract encryption techniques;
- services for auditing and logging interactions and security violations;
- services for identification;
- services for authentication;
- services for authorization;
- services for intrusion detection and prevention;
- services for availability including support for quality of service specifications and metrics.

Access Control Policies specializes capabilities architecturally implied by its associated concepts of Artifact, Change, Composition, Interaction, Interoperability, Metrics, Policy, PolicyAndContract, PolicyAndContractLanguage. The implied architectural capabilities are described in the following paragraphs.

Artifact

An artifact is a managed resource within the Semantic Infrastructure.

An artifact is associated with the following capabilities:
• descriptions to enable the artifact to be visible, where the description includes a unique identifier for the artifact and a sufficient, and preferably a machine processible, representation of the meaning of terms used to describe the artifact, its functions, and its effects;
• one or more discovery mechanisms that enable searching for artifacts that best meet the search criteria specified by the service participant; where the discovery mechanism will have access to the individual artifact descriptions, possibly through some repository mechanism;
• accessible storage of artifacts and artifact descriptions, so service participants can access, examine, and use the artifacts as defined.

Change Artifact descriptions change over time and their contents will reflect changing needs and context. Architectural implications of change on the Semantic Infrastructure are reflected in the following capabilities:
• mechanisms to support the storage, referencing, and access to normative definitions of one or more versioning schemes that may be applied to identify different aggregations of descriptive information, where the different schemes may be versions of a versioning scheme itself;
• configuration management mechanisms to capture the contents of the each aggregation and apply a unique identifier in a manner consistent with an identified versioning scheme;
• one or more mechanisms to support the storage, referencing, and access to conversion relationships between versioning schemes, and the mechanisms to carry out such conversions.

Composition Artifact Descriptions may capture very focused information subsets or can be an aggregate of numerous component descriptions. Service description is an example of a likely aggregate for which manual maintenance of all aspects would not be feasible. Architectural implications of composition on the Semantic Infrastructure are reflected in the following capabilities:
• tools to facilitate identifying description elements that are to be aggregated to assemble the composite description;
• tools to facilitate identifying the sources of information to associate with the description elements;
• tools to collect the identified description elements and their associated sources into a standard, referenceable format that can support general access and understanding;
• tools to automatically update the composite description as the component sources change, and to consistently apply versioning schemes to identify the new description contents and the type and significance of change that occurred.

Interaction Descriptions of interactions are important for enabling auditability and repeatability, thereby establishing a context for results and support for understanding observed change in performance or results. Infrastructure services provide mechanisms to support service interaction. Architectural implications of interactions on the Semantic Infrastructure are reflected in the following capabilities:
• one or more mechanisms to capture, describe, store, discover, and retrieve interaction logs, execution contexts, and the combined interaction descriptions;
• one or more mechanisms for attaching to any results the means to identify and retrieve the interaction description under which the results were generated.
• mediation services such as message and event brokers, providers, and/or buses that provide message translation/ transformation, gateway capability, message persistence, reliable message delivery, and/or intelligent routing semantics;
• binding services that support translation and transformation of multiple application-level protocols to standard network transport protocols;
• auditing and logging services that provide a data store and mechanism to record information related to service interaction activity such as message traffic patterns, security violations, and service contract and policy violations;
• security services that abstract techniques such as public key cryptography, secure networks, virus protection, etc., which provide protection against common security threats in a SOA ecosystem;
• monitoring services such as hardware and software mechanisms that both monitor the performance of systems that host services and network traffic during service interaction, and are capable of generating regular monitoring reports.

Interoperability Descriptions provide up-to-date information on what a resource is, the conditions for interacting with the resource, and the results of such interactions. As such, the description is the source of vital information in establishing willingness to interact with a resource, reachability to make interaction possible, and compliance with relevant conditions of use. Architectural implications of interoperability on the Semantic Infrastructure are reflected in the following capabilities:
• one or more discovery mechanisms that enable searching for described resources that best meet the criteria specified by a service participant, where the discovery mechanism will have access to individual descriptions, possibly through some repository mechanism;
• tools to appropriately track users of the descriptions and notify them when a new version of the description is available.

Metrics Artifact Descriptions include references to metrics which describe the operational characteristics of the subjects being described
Architectural implications of metrics on the Semantic Infrastructure are reflected in the following capabilities:
• access to platform infrastructure monitoring and reporting capabilities
• access to metrics information generated or accessible by related services
• mechanisms to catalog and enable discovery of which metrics are available for a described artifact and information on how these metrics can be accessed;
• mechanisms to catalog and enable discovery of compliance records associated with policies, contracts, and constraints that are based on these metrics.

Policy Artifact Descriptions include references to policies defining conditions of use and optionally contracts representing agreement on policies and other conditions. Architectural implications of policy on the Semantic Infrastructure are reflected in the following capabilities:
• descriptions to enable the policy modules to be visible, where the description includes a unique identifier for the policy and a sufficient, and preferably a machine processible, representation of the meaning of terms used to describe the policy, its functions, and its effects;
• one or more discovery mechanisms that enable searching for policies that best meet the search criteria specified by the service participant; where the discovery mechanism will have access to the individual policy descriptions, possibly through some repository mechanism;
• accessible storage of policies and policy descriptions, so service participants can access, examine, and use the policies as defined.
Policy capabilities are specialization of Artifact capabilities.

**PolicyAndContract** While policy and contract descriptions have much of the same architectural implications as Service Descriptions, mechanisms supporting policies and contracts also have the following architectural implications:

- decision procedures which must be able to measure and render decisions on constraints;
- enforcement of decisions;
- measurement and notification of obligation constraints;
- auditablety of decisions, enforcement, and obligation measurements;
- administration of policy and contract language artifacts;
- storage of policies and contracts;
- distribution of policies/contracts;
- conflict resolution or elevation of conflicts in policy rules;
- delegation of policy authority to agents acting on behalf of a client;
- decision procedures capable of incorporating roles and/or attributes for rendered decisions.

**PolicyAndContractLanguage** While policy and contract descriptions have much of the same architectural implications as Service Descriptions, languages supporting policies and contracts also have the following architectural implications:

- expression of assertion and commitment policy constraints;
- expression of positive and negative policy constraints;
- expression of permission and obligation policy constraints;
- nesting of policy constraints allowing for abstractions and refinements of a policy constraint;
- definition of alternative policy constraints to allow for the selection of compatible policy constraints for a consumer and provider;
- composition of policies to combine one or more policies.

**Capabilities**

- accessContolPolicyModel
- assembly
- binding
- complianceDiscovery
- componentAcquisition
- compositionArchive
- compositionChange
- configurationManagement
- discovery
- identity
- interactionLog
- interactionResults
- interoperabilityDiscovery
- logging
- mediation
- metadata
- metrics
- metricsDiscovery
- monitor
- monitoring
- policyAdministration
- policyAlternative
- policyAssertion
- policyAudit
- policyAuthorityDelegation
- policyComposition
- policyConflictResolution
- policyConstraint
- policyDecision
- policyDecisionProcedures
- policyDistribution
- policyEnforcement
- policyMetrics
- policyObligation
- policyRefinement
- policyStore
- provenance
- security
- serviceChangeNotification
- store
- transition
- versioning

**Requirements traceability**

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Source</th>
<th>Capability</th>
</tr>
</thead>
<tbody>
<tr>
<td>There is a need to manage access control and other applicable types of control for the repository. Note that “other applicable types of control” is to be defined later in the PIM and PSM.</td>
<td>Gap Analysis:: HL7 CIC::C1-C4</td>
<td>accessContolPolicyModel</td>
</tr>
</tbody>
</table>
Service Oriented Architecture is an architectural paradigm for organizing and utilizing distributed capabilities that may be under the control of different ownership domains. Consequently, it is important that organizations that plan to engage in service interactions adopt governance policies and procedures so that there is standardization across both internal and external boundaries. The aim is to promote the effective creation and use of SOA-based services. SOA governance requires numerous architectural capabilities on the Semantic Infrastructure: Governance is exercised through policies and assumes multiple use of focused policy modules that can be employed across many common circumstances. This is elaborated in the inherited Policy profile. Governance requires that the participants understand the intent of governance, the structures created to define and implement governance, and the processes to be followed to make governance operational. This is provided by capabilities specialized from the inherited Management Profile. Governance policies are made operational through rules and regulations. This is provided by the following capabilities, most of which are specializations of the inherited Artifact Profile: * descriptions to define the rules and regulations to be visible, where the description includes a unique identifier and a sufficient, and preferably a machine processable, representation of the meaning of terms used to describe the rules and regulations; * one or more discovery mechanisms that enable searching for rules and regulations that may apply to situations corresponding to the search criteria specified by the service participant; where the discovery mechanism will have access to the individual descriptions of rules and regulations, possibly through some repository mechanism; * accessible storage of rules and regulations and their respective descriptions, so service participants can understand and prepare for compliance, as defined. * SOA services to access and execute theses rules and regulations. This is elaborated in the inherited Management profile. Governance relies on metrics to define and measure compliance. This is elaborated in the inherited Managed profile.

Interaction is the activity involved in using a service to access capability in order to achieve a particular desired real world effect, where real world effect is the actual result of using a service. An interaction can be characterized by a sequence of actions. Consequently, interacting with a service, i.e. performing actions against the service, results in the exchange of messages. Interacting with Services has the following architectural implications that facilitate service interaction: * A well-defined specific Information Model, as elaborated in the inherited Information Model profile. A well-defined service Behavior Model, as elaborated in the inherited Behavior Model profile. Service composition mechanisms to support creation of service-oriented business processes: * choreography of service-oriented collaborations, as elaborated in the inherited Service Composition profile. Infrastructure services that provide mechanisms to support service interaction, as elaborated in the inherited interaction profile. A layered and tiered service component architecture that supports multiple message exchange patterns (MPEX), as elaborated in the inherited Message Exchange profile.

Artifact Descriptions include references to policies defining conditions of use and optionally contracts representing agreement on policies and other conditions. Architectural implications of policy on the Semantic Infrastructure are reflected in the following capabilities: * descriptions to enable the policy module to be visible, where the description includes a unique identifier for the policy and a sufficient, and preferably a machine processable, representation of the meaning of terms used to describe the policy, its functions, and its effects; * one or more discovery mechanisms that enable searching for the policies that best meet the search criteria specified by the service participant; where the discovery mechanism will have access to the individual policy descriptions, possibly through some repository mechanism; * accessible storage of policies and policy descriptions, so service participants can access, examine, and use the policies as defined. Policy capabilities are specialization of Artifact capabilities.

A service description is an artifact, usually document-based, that defines or references information needed to use, deploy, manage and otherwise control a service. This includes not only the information and behavior models associated with a service to define the service interface but also includes information needed to decide whether the service is appropriate for the current needs of the service consumer. Thus, the service description will also include information such as service reachability, service functionality, and the policies and contracts associated with a service. A service description artifact may be a single document or it may be an interlinked set of documents. Architectural implications of service description on the Semantic Infrastructure are reflected in the following functional decomposition: * Description will change over time and its contents will reflect changing needs and context. This is elaborated in the inherited Change profile. * Description makes use of defined semantics, where the semantics may be used for categorization or providing other property and value information for description classes. This is elaborated in the inherited Semantic profile. * Descriptions include reference to policies defining conditions of use and optionally contracts representing agreement on policies and other conditions. This is elaborated in the inherited Policy profile. * Descriptions include reference to services which describe the operational characteristics of the subjects being described. This is elaborated in the inherited Service profile. * Descriptions of the interface, including capability, reliability, and performance characteristics, are understood. Service discovery and matchmaking, according to observed change in performance or results. This is elaborated in the inherited Interaction profile. * Descriptions may capture very focused information. Such as, an aggregate of numerous service component descriptions organizing the service component descriptions. An aggregate of which manual maintenance of all aspects would not be feasible. This is elaborated in the inherited Composition profile. * Descriptions provide up-to-date information on what a resource is, the conditions for interacting with the resource, and the results of such interactions. As such, the description is the source of vital information in establishing willingness to interact with a resource, reachability to make interaction possible, and compliance with relevant conditions of use. This is elaborated in the inherited Interoperability profile. Service policies capability are specialization of Artifact capabilities.

Service policies help establish constraints on the service specifications and mandate an approach. Policies can be specified around governance, access control and other design and runtime constraints.

One of the key requirements for participants interacting with each other in the context of a SOA is achieving visibility before services can interoperate. The participants need to be visible to each other. The participants need visibility in terms of awareness, willingness, and reachability. Visibility in a SOA ecosystem has the following architectural implications on mechanisms: providing awareness for determining willingness to interact will require support for: * verification of identity and credentials of the provider and/or consumer; * access to and understanding of description; * inspection of functionality, and capability mechanisms to support such interaction. The architectural implications for mechanisms to support such interaction will require support for: * the location or address of an endpoint; verification and use of a service interface by means of a communication protocol; * determination of presence with an endpoint which may only be determined at the point interaction but may be further aided by the use of a presence protocol for which the provider is enabled. This is elaborated in the inherited Interaction profile.

Service governance includes the policies and contracts to support SOA governance. The policies and contracts are reflected in the following functional decomposition: * creation of Description preferably conforming to a standard Description format and structure; * publishing of Description directly to a repository; * versioning of Description; * publishing and distribution of Description to a repository; * publishing of Description to a service registry. This is elaborated in the inherited Policy profile. Policies associated with SOA services are defined as services and resources. This is elaborated in the inherited Policy profile.

Service discovery in an SOA ecosystem is a discovery mechanism to facilitate service location. This is elaborated in the inherited Discovery profile.
accessContolPolicyModel

Description
Access Control Policy Model with capabilities to create, destroy, edit, maintain access control policy descriptions.

Requirements addressed
- CIC-4 - Provide controlled, secured access to stored data
- Service Policies
- Specification Content

Overview of possible operations

assembly

Description
Tools to facilitate identifying description elements that are to be aggregated to assemble the composite description.

Requirements addressed
- Service Description Model

Overview of possible operations

binding

Description
binding services that support translation and transformation of multiple application-level protocols to standard network transport protocols;

Requirements addressed
- Interacting with Services Model

Overview of possible operations

complianceDiscovery

Description
Mechanisms to catalog and enable discovery of compliance records associated with policies, contracts, and constraints that are based on these metrics.

Requirements addressed
- Service Description Model

Overview of possible operations

componentAcquisition

Description
Tools to facilitate identifying the sources of information to associate with the description elements.

Requirements addressed
- Service Description Model

Overview of possible operations

compositionArchive

Description
Tools to collect the identified description elements and their associated sources into a standard, referenceable format that can support general access and understanding.

Requirements addressed
- Service Description Model

Overview of possible operations
compositionChange

Description
Tools to automatically update the composite description as the component sources change, and to consistently apply versioning schemes to identify the new description contents and the type and significance of change that occurred.

Requirements addressed
- Service Description Model

Overview of possible operations

configurationManagement

Description
Mechanisms to support the storage, referencing, and access to normative definitions of one or more versioning schemes that may be applied to identify different aggregations of descriptive information, where the different schemes may be versions of a versioning scheme itself.

Requirements addressed
- Service Description Model

Overview of possible operations

discovery

Description
One or more discovery mechanisms that enable searching for artifacts that best meet the search criteria specified by the service participant; where the discovery mechanism will have access to the individual artifact descriptions, possibly through some repository mechanism.

Requirements addressed
- Service Visibility Model
- Service Description Model
- Governance Model

Overview of possible operations

identity

Description
Descriptions which include a unique identifier for the artifact.

Requirements addressed
- Governance Model
- Service Description Model

Overview of possible operations

interactionLog

Description
One or more mechanisms to capture, describe, store, discover, and retrieve interaction logs, execution contexts, and the combined interaction descriptions.

Requirements addressed
- Service Description Model
- Interacting with Services Model

Overview of possible operations

interactionResults

Description
One or more mechanisms for attaching to any results the means to identify and retrieve the interaction description under which the results were generated.

Requirements addressed
- Interacting with Services Model
Service Description Model

Overview of possible operations

interoperability

Description

One or more discovery mechanisms that enable searching for described resources that best meet the criteria specified by a service participant, where the discovery mechanism will have access to individual descriptions, possibly through some repository mechanism.

Requirements addressed

- Service Description Model

logging

Description

Auditing and logging services that provide a data store and mechanism to record information related to service interaction activity such as message traffic patterns, security violations, and service contract and policy violations.

Requirements addressed

- Interacting with Services Model

mediation

Description

Mediation services such as message and event brokers, providers, and/or buses that provide message translation/ transformation, gateway capability, message persistence, reliable message delivery, and/or intelligent routing semantics.

Requirements addressed

- Interacting with Services Model

metadata

Description

A representation of the meaning of terms used to describe the artifact, its functions, and its effects.

Requirements addressed

- Governance Model
- Service Description Model

metrics

Description

Access to metrics information generated or accessible by related services.

Requirements addressed

- Service Description Model
- Governance Model

metricsDiscovery

Description

Mechanisms to catalog and enable discovery of which metrics are available for a described artifact and information on how these metrics can be accessed.

Requirements addressed


• **Service Description Model**

Overview of possible operations

monitor

Description

Access to platform infrastructure monitoring and reporting capabilities.

Requirements addressed

• **Service Description Model**
  • **Governance Model**

Overview of possible operations

monitoring

Description

monitoring services such as hardware and software mechanisms that both monitor the performance of systems that host services and network traffic during service interaction, and are capable of generating regular monitoring reports.

Requirements addressed

• **Interacting with Services Model**

Overview of possible operations

policyAdministration

Description

Administration of policy and contract language artifacts.

Requirements addressed

• **Policies and Contracts Model**

Overview of possible operations

policyAlternative

Description

Definition of alternative policy constraints to allow for the selection of compatible policy constraints for a consumer and provider.

Requirements addressed

• **Policies and Contracts Model**

Overview of possible operations

policyAssertion

Description

Expression of assertion and commitment policy constraints.

Requirements addressed

• **Policies and Contracts Model**

Overview of possible operations

policyAudit

Description

Auditability of decisions, enforcement, and obligation measurements.

Requirements addressed

• **Policies and Contracts Model**

Overview of possible operations
policyAuthorityDelegation

Description
Delegation of policy authority to agents acting on behalf of a client.

Requirements addressed
- Policies and Contracts Model

Overview of possible operations

policyComposition

Description
Composition of policies to combine one or more policies.

Requirements addressed
- Policies and Contracts Model

Overview of possible operations

policyConflictResolution

Description
Conflict resolution or elevation of conflicts in policy rules.

Requirements addressed
- Policies and Contracts Model

Overview of possible operations

policyConstraint

Description
Expression of positive and negative policy constraints.

Requirements addressed
- Policies and Contracts Model

Overview of possible operations

policyDecision

Description
Decision procedures which must be able to measure and render decisions on constraints.

Requirements addressed
- Policies and Contracts Model

Overview of possible operations

policyDecisionProcedures

Description
Decision procedures capable of incorporating roles and/or attributes for rendered decisions.

Requirements addressed
- Policies and Contracts Model

Overview of possible operations

policyDistribution

Description
Distribution of policies/contracts.
Requirements addressed
• Policies and Contracts Model
Overview of possible operations

policyEnforcement
Description
Enforcement of decisions.
Requirements addressed
• Policies and Contracts Model
Overview of possible operations

policyMetrics
Description
Measurement and notification of obligation constraints.
Requirements addressed
• Policies and Contracts Model
Overview of possible operations

policyObligation
Description
Expression of permission and obligation policy constraints.
Requirements addressed
• Policies and Contracts Model
Overview of possible operations

policyRefinement
Description
Nesting of policy constraints allowing for abstractions and refinements of a policy constraint.
Requirements addressed
• Policies and Contracts Model
Overview of possible operations

policyStore
Description
Storage of policies and contracts.
Requirements addressed
• Policies and Contracts Model
Overview of possible operations

provenance
Description
While the Resource identity provides the means to know which subject and subject description are being considered, Provenance as related to the Description class provides information that reflects on the quality or usability of the subject. Provenance specifically identifies the entity (human, defined role, organization, ...) that assumes responsibility for the resource being described and tracks historic information that establishes a context for understanding what the resource provides and how it has changed over time. Responsibilities may be directly assumed by the Stakeholder who owns a Resource or the Owner may designate Responsible Parties for the various aspects of maintaining the resource and provisioning it for use by others. There
may be more than one entity identified under Responsible Parties; for example, one entity may be responsible for code maintenance while another is responsible for provisioning of the executable code. The historical aspects may also have multiple entries, such as when and how data was collected and when and how it was subsequently processed, and as with other elements of description, may provide links to other assets maintained by the Resource owner.

Requirements addressed
Overview of possible operations

security
Description
security services that abstract techniques such as public key cryptography, secure networks, virus protection, etc., which provide protection against common security threats in a SOA ecosystem;

Requirements addressed
  • Interacting with Services Model

Overview of possible operations

serviceChangeNotification
Description
Tools to appropriately track users of the descriptions and notify them when a new version of the description is available.

Requirements addressed
  • Service Description Model

Overview of possible operations

store
Description
Accessible storage of artifacts and artifact descriptions, so service participants can access, examine, and use the artifacts as defined.

Requirements addressed
  • Service Description Model
  • Governance Model

Overview of possible operations

transition
Description
One or more mechanisms to support the storage, referencing, and access to conversion relationships between versioning schemes, and the mechanisms to carry out such conversions.

Requirements addressed
  • Service Description Model

Overview of possible operations

versioning
Description
Configuration management mechanisms to capture the contents of the each aggregation and apply a unique identifier in a manner consistent with an identified versioning scheme.

Requirements addressed
  • Service Description Model

Overview of possible operations