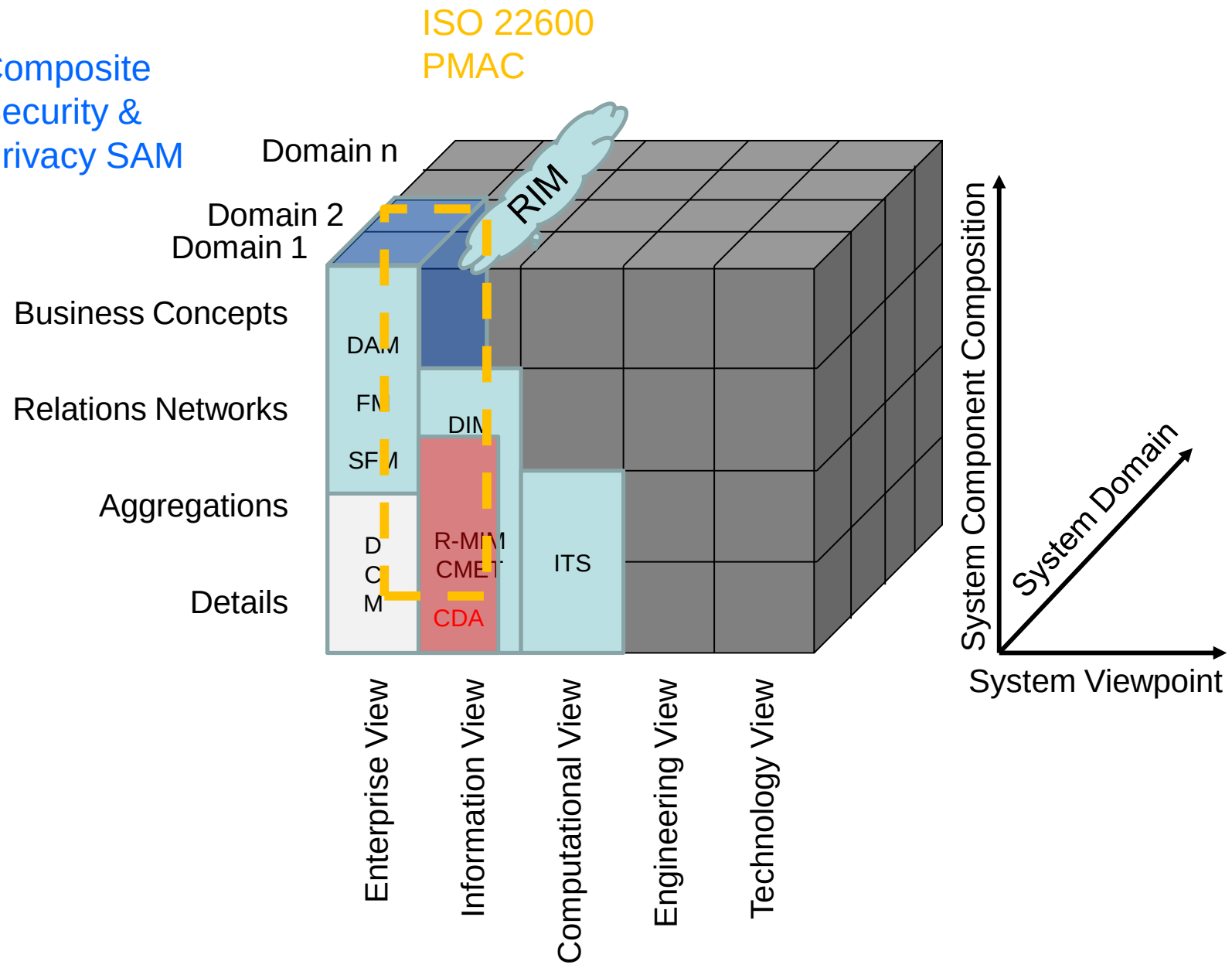
Implications of SOA Architectures for Security and Privacy

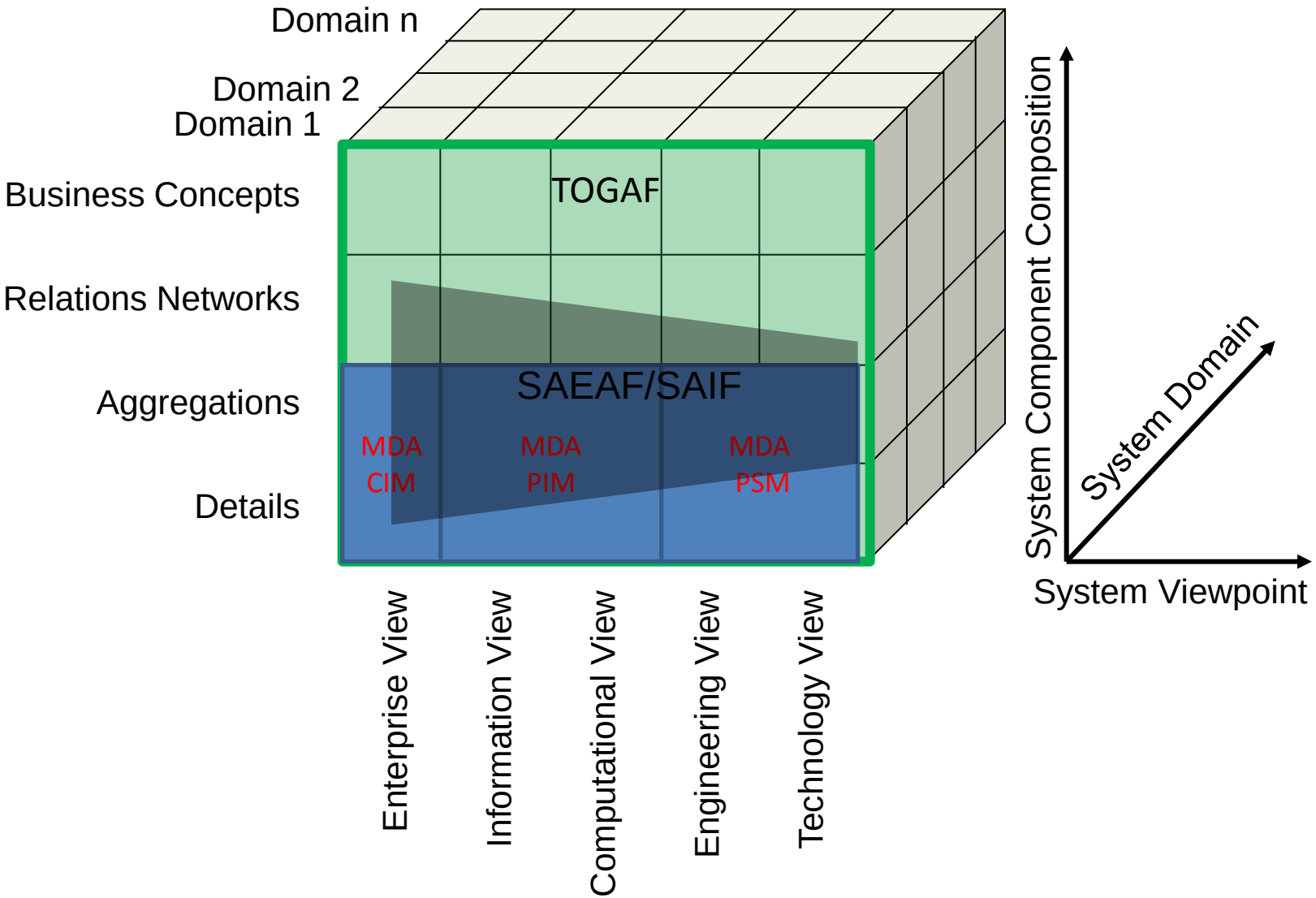
Bernd Blobel, PhD, FACMI, FACHI, FHL7

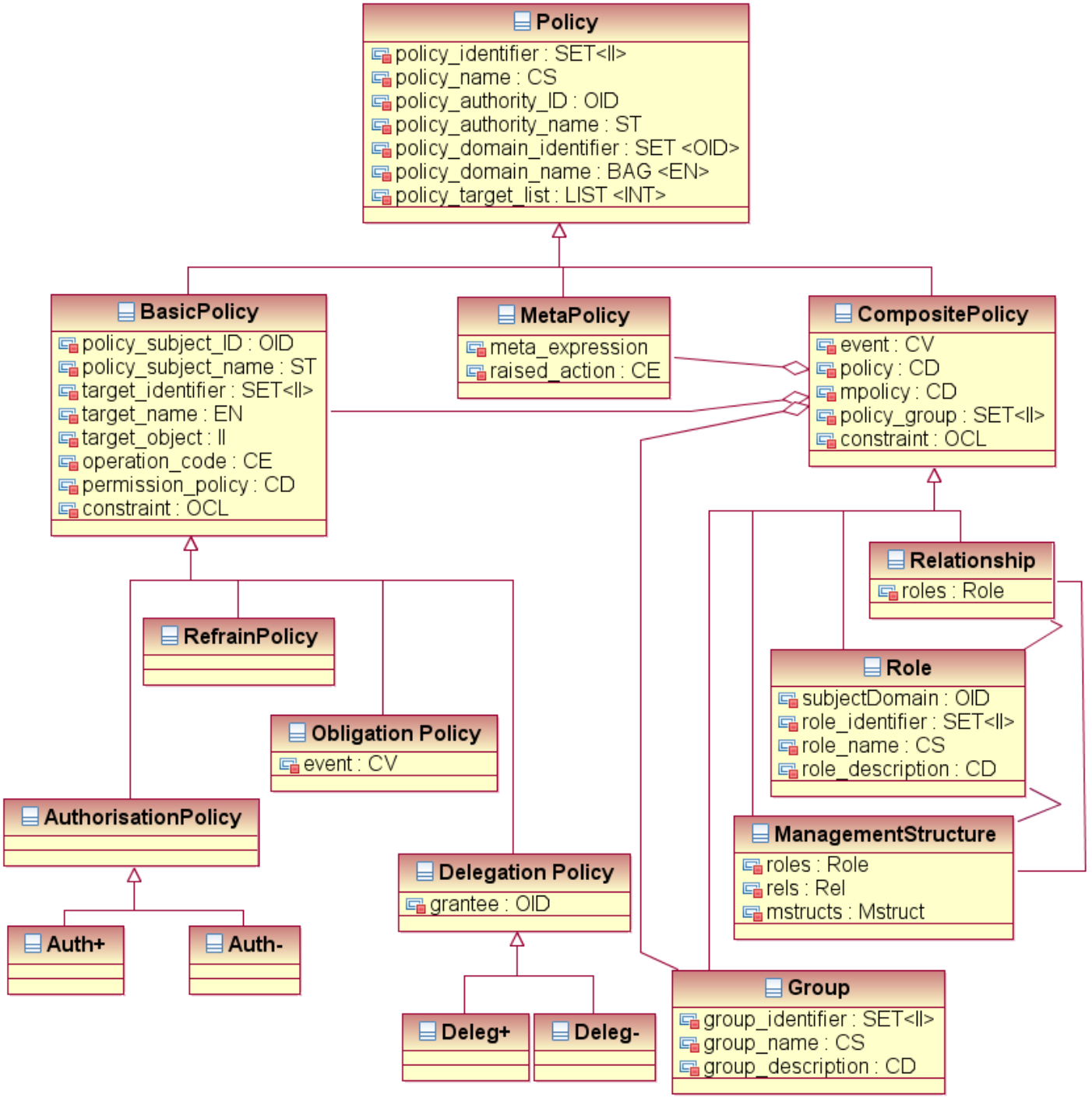
eHealth Competence Center Regensburg

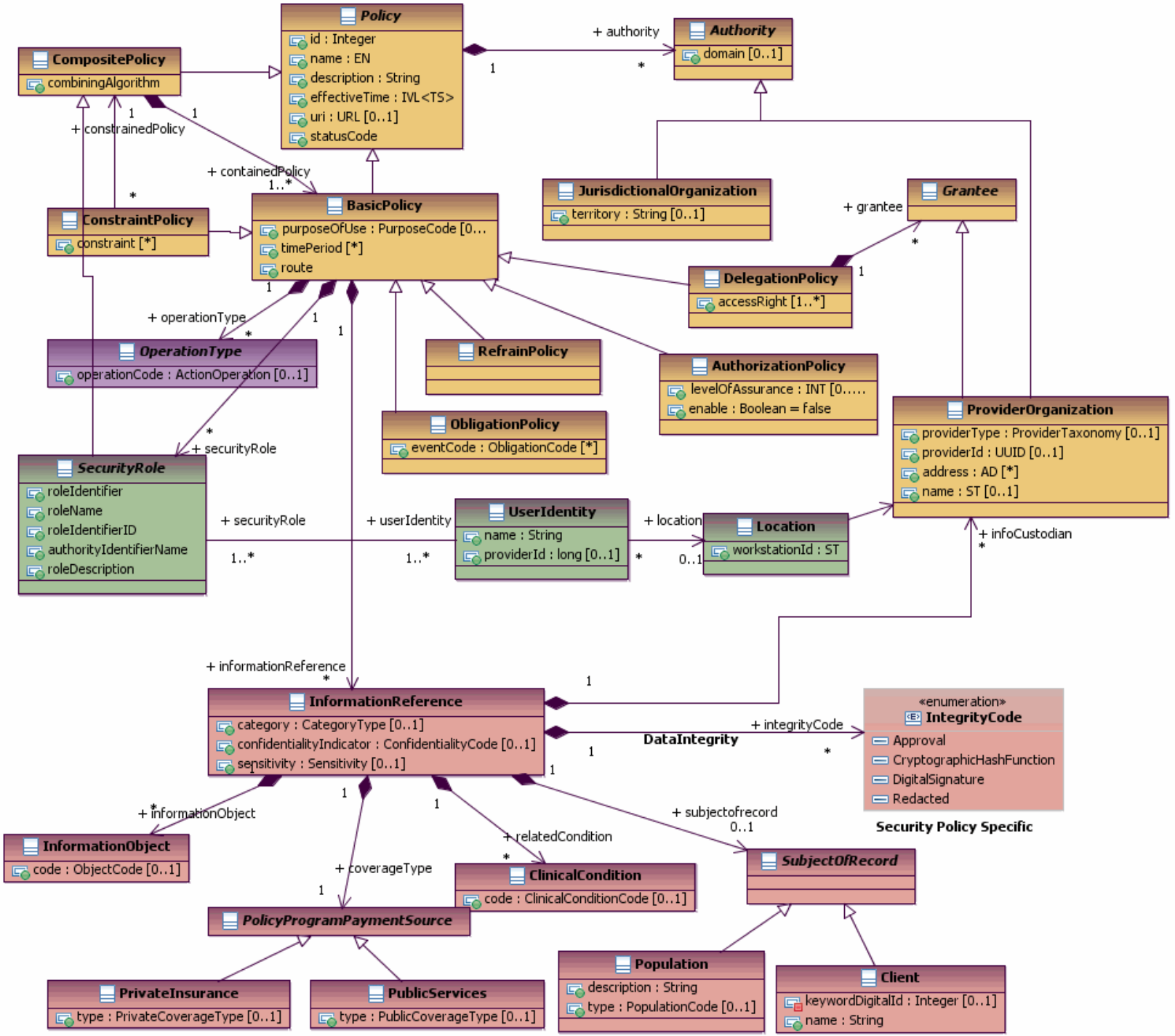
Composite Security & Privacy SAM

ISO 22600
PMAC




Domain n
Domain 2
Domain 1
Business Concepts
Relations Networks
Aggregations
Details
TOGAF
SAEAF/SAIF
MDA
CIM
MDA
PIM
MDA
PSM
Enterprise View
Information View
Computational View
Engineering View
Technology View
System Component Composition
System Domain
System Viewpoint


Policy
policy_identifier : SET<II>
policy_name : CS
policy_authority_ID : OID
policy_authority_name : ST
policy_domain_identifier : SET <OID>
policy_domain_name : BAG <EN>
policy_target_list : LIST <INT>
BasicPolicy
policy_subject_ID : OID
policy_subject_name : ST
target_identifier : SET<II>
target_name : EN
target_object : II
operation_code : CE
permission_policy : CD
constraint : OCL
MetaPolicy
meta_expression
raised_action : CE
CompositePolicy
event : CV
policy : CD
mpolicy : CD
policy_group : SET<II>
constraint : OCL
Relationship
roles : Role
RefrainPolicy
Role
subjectDomain : OID
role_identifier : SET<II>
role_name : CS
role_description : CD
Obligation Policy
event : CV
ManagementStructure
roles : Role
rels : Rel
mstructs : Mstruct
AuthorisationPolicy
Delegation Policy
grantee : OID
Auth+
Auth-
Group
group_identifier : SET<II>
group_name : CS
group_description : CD
Deleg+
Deleg-


Policy
id : Integer
name : EN
description : String
effectiveTime : IVL<TS>
uri : URL [0..1]
statusCode
CompositePolicy
combiningAlgorithm
+ constrainedPolicy
+ containedPolicy
+ authority
Authority
domain [0..1]
JurisdictionalOrganization
territory : String [0..1]
Grantee
+ grantee
ConstraintPolicy
constraint [*]
BasicPolicy
purposeOfUse : PurposeCode [0...
timePeriod [*]
route
DelegationPolicy
accessRight [1..*]
+ operationType
OperationType
operationCode : ActionOperation [0..1]
RefrainPolicy
AuthorizationPolicy
levelOfAssurance : INT [0.....
enable : Boolean = false
ObligationPolicy
eventCode : ObligationCode [*]
ProviderOrganization
providerType : ProviderTaxonomy [0..1]
providerId : UUID [0..1]
address : AD [*]
name : ST [0..1]
+ securityRole
SecurityRole
roleIdentifier
roleName
roleIdentifierID
authorityIdentifierName
roleDescription
+ userIdentity
UserIdentity
name : String
providerId : long [0..1]
+ location
Location
workstationId : ST
+ infoCustodian
+ informationReference
InformationReference
category : CategoryType [0..1]
confidentialityIndicator : ConfidentialityCode [0..1]
sensitivity : Sensitivity [0..1]
DataIntegrity
+ integrityCode
«enumeration»
IntegrityCode
Approval
CryptographicHashFunction
DigitalSignature
Redacted
Security Policy Specific
+ informationObject
InformationObject
code : ObjectCode [0..1]
+ coverageType
+ relatedCondition
ClinicalCondition
code : ClinicalConditionCode [0..1]
+ subjectofrecord
SubjectOfRecord
PolicyProgramPaymentSource
PrivateInsurance
type : PrivateCoverageType [0..1]
PublicServices
type : PublicCoverageType [0..1]
Population
description : String
type : PopulationCode [0..1]
Client
keywordDigitalId : Integer [0..1]
name : String

Used Architectural Specifications

- OASIS Reference Model for SOA,
- **OASIS Reference Architecture for SOA Foundation,**
- OMG SoaML Specification,
- The Open Group SOA Ontology,
- The Open Group SOA Reference Architecture,
- The Open Group SOA Governance Framework, and
- The Open Group Service Integration Maturity Model.

Architectural Implications of Service Description on the SOA Ecosystem

- Descriptions include reference to policies defining conditions of use and optionally contracts representing agreement on policies and other conditions. This requires the existence of (as also enumerated under governance):
  - 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.**

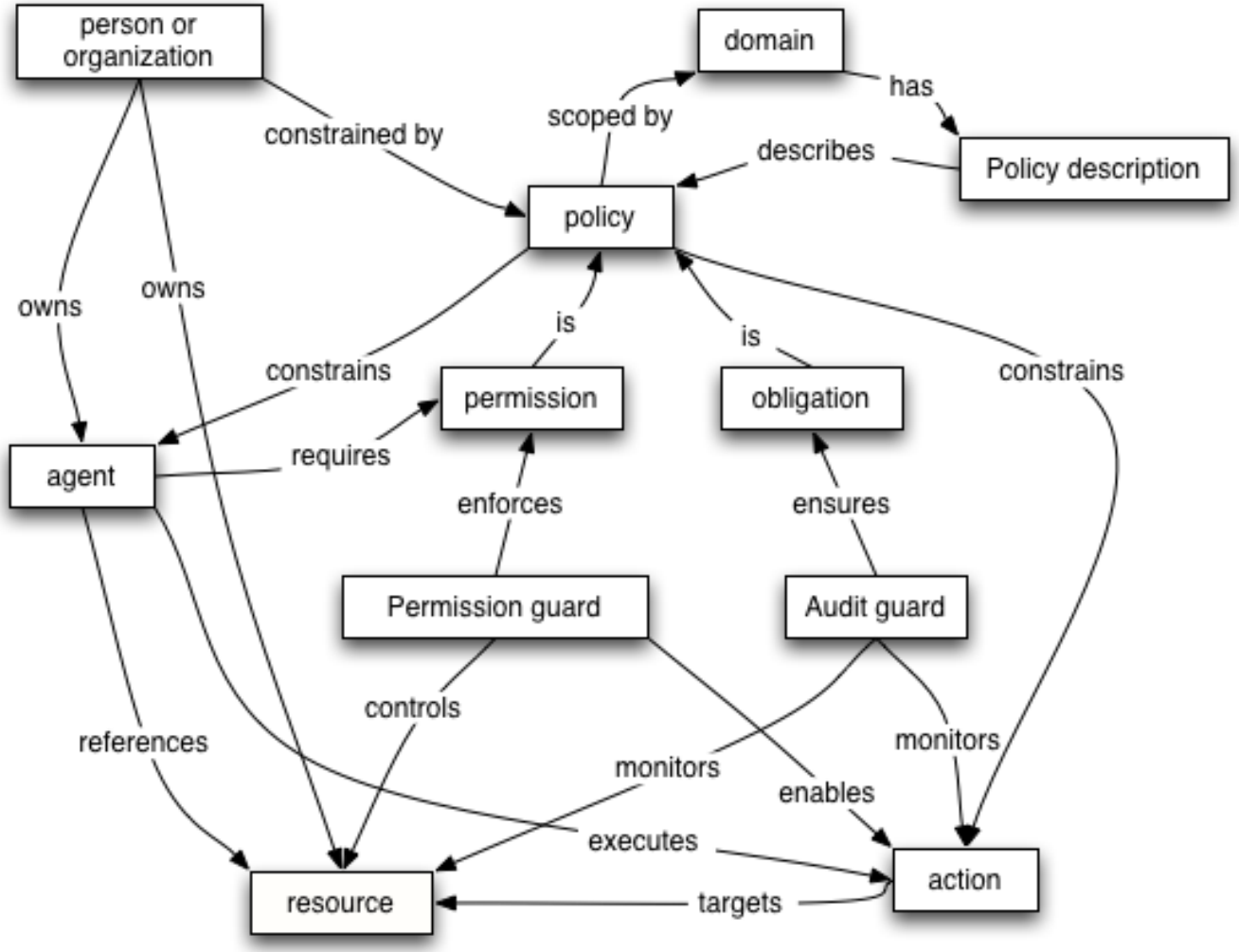
- Descriptions of the interactions are important for enabling auditability and repeatability, thereby establishing a context for results and support for understanding observed change in performance or results. This requires the existence of:
  - one or more mechanisms to capture, describe, store, discover, 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.

Architectural Implications of Visibility in a SOA Ecosystem on Mechanisms Providing Support for Awareness, Willingness, and Reachability

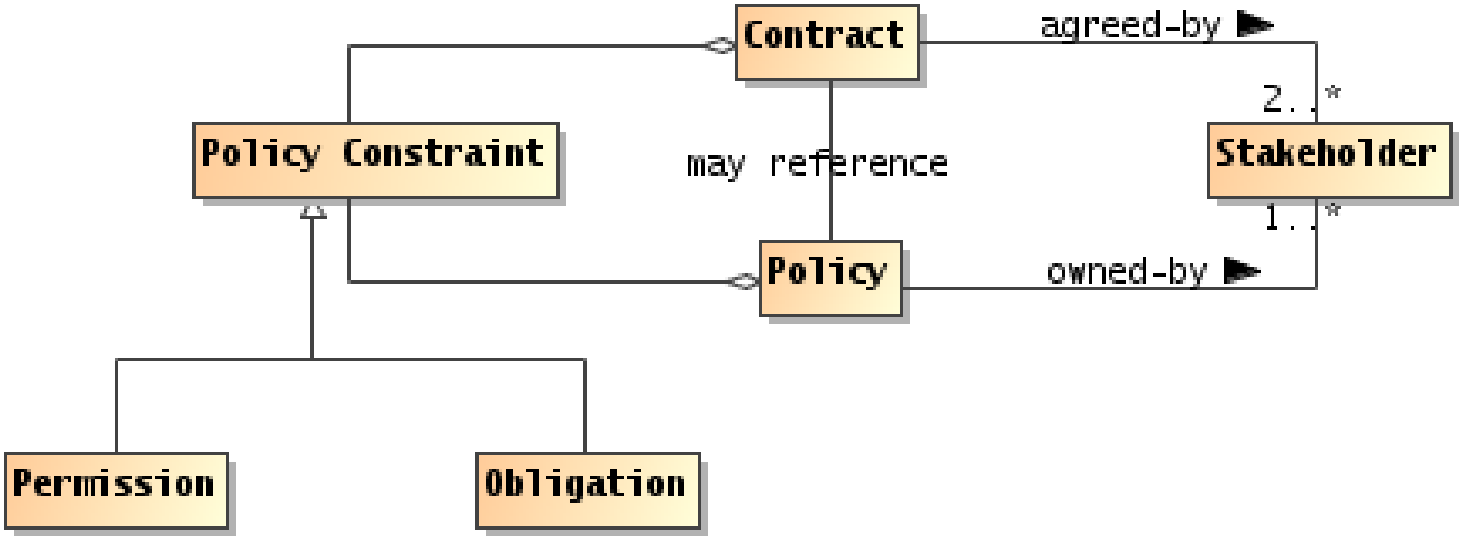
- In a SOA ecosystem with complex **social structures, awareness may be provided** for specific communities of interest. The architectural mechanisms for providing awareness to communities of interest will require support for:
  - policies that allow dynamic formation of communities of interest;
  - trust that awareness can be provided for and only for specific communities of interest, the bases of which is typically built on keying and encryption technology.
- The architectural mechanisms 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 capabilities;
  - inspection of policies and/or contracts.

Architectural Implications of Interacting with Services

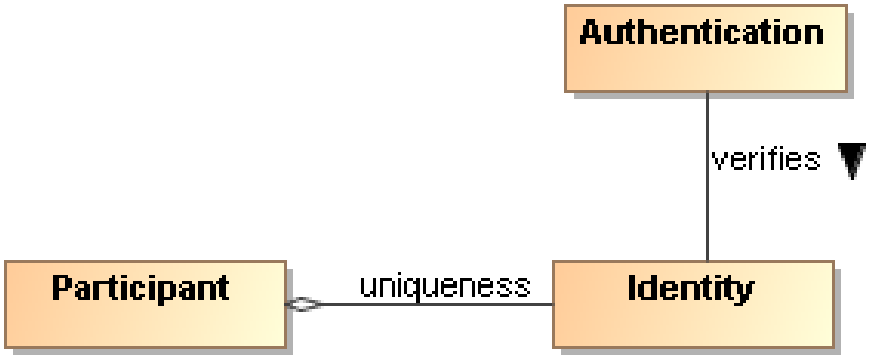
- Infrastructure services that provides mechanisms to support service interaction, including but not limited to:
  - auditing and logging services that provide a data store and mechanism to record information related to service interaction activity such as message traffic patterns, security violations, 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;


person or organization
domain
has
scoped by
constrained by
describes
Policy description
policy
owns
owns
is
is
constrains
constrains
permission
obligation
agent
requires
enforces
ensures
Permission guard
Audit guard
controls
references
monitors
monitors
enables
executes
action
resource
targets

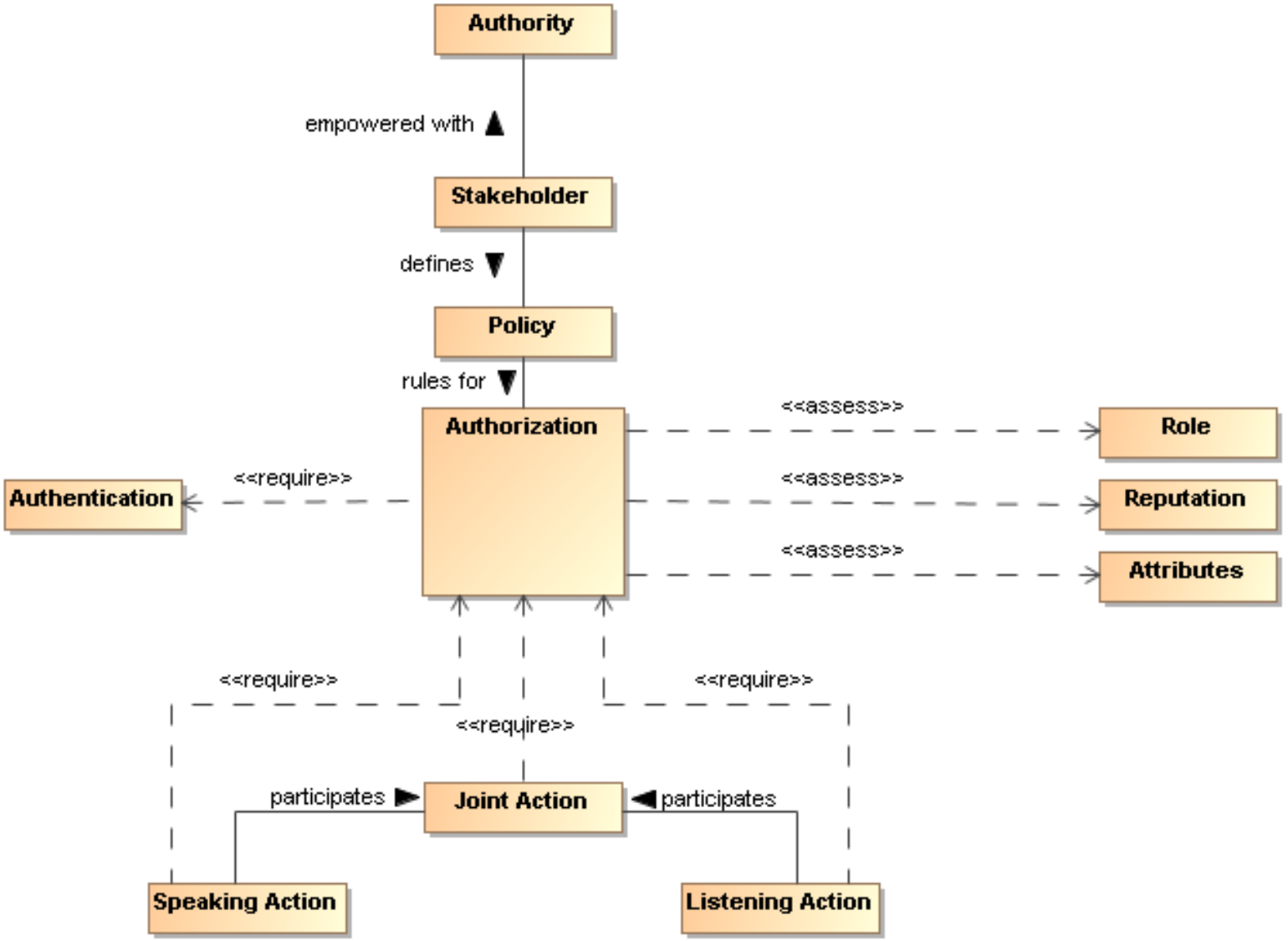
Policies and Contracts



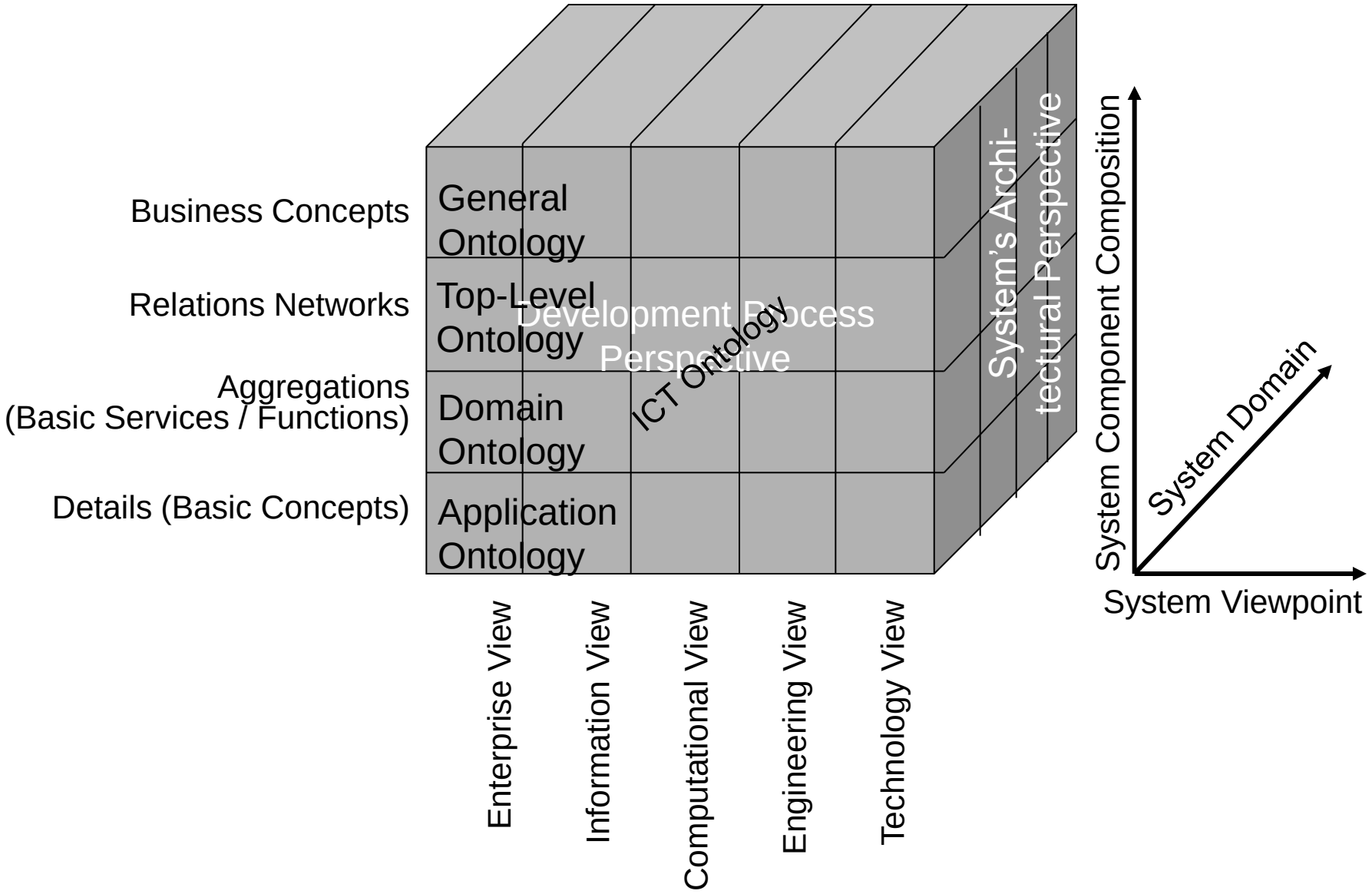
Authentication



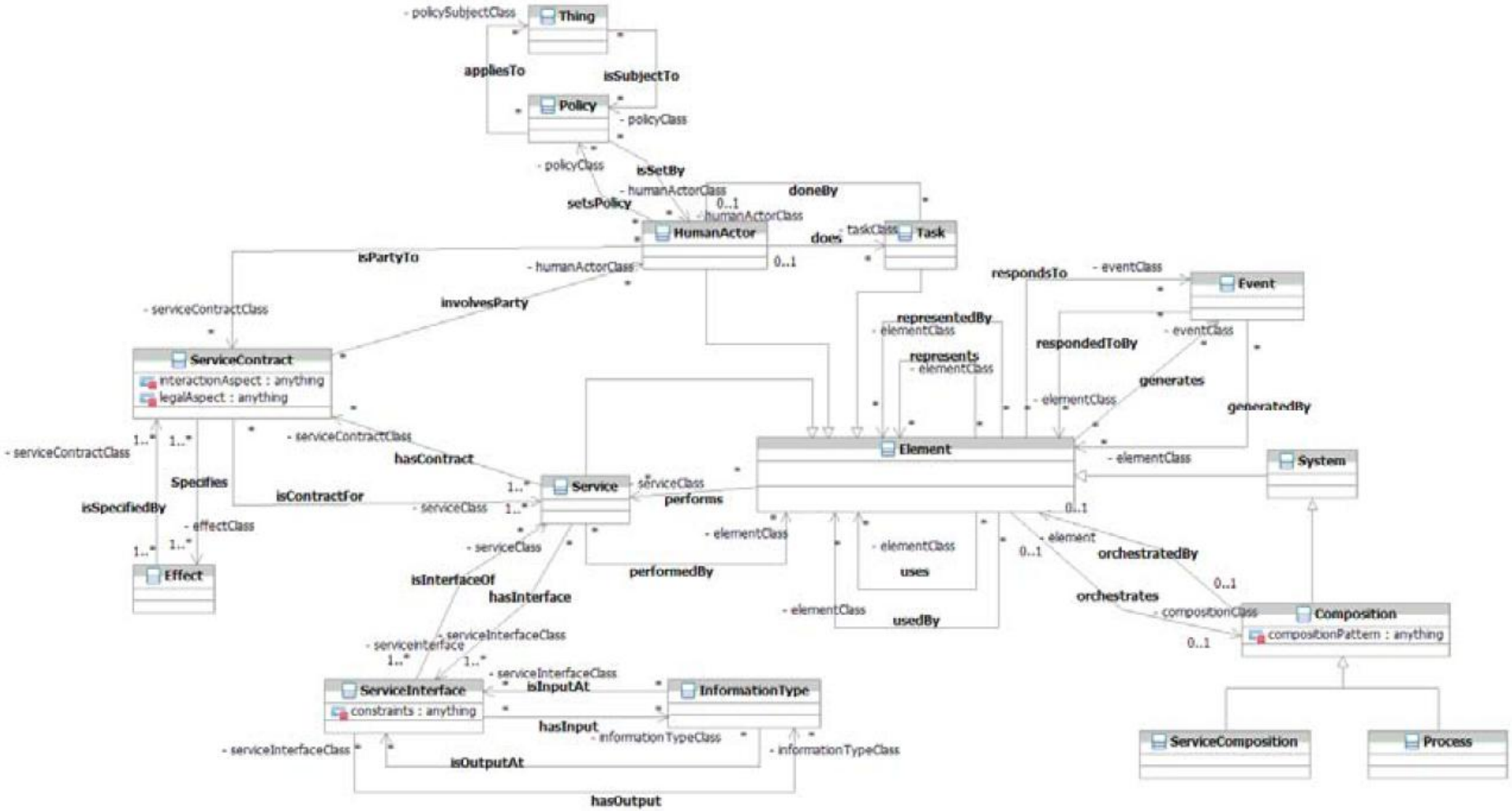
Authorization



Designing Ontology Systems with the GCM



SOA Ontology



Architectural Implications of SOA Governance

- Governance is expressed through policies and assumes multiple use of focused policy modules that can be employed across many common circumstances. This requires the existence of:
  - 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 process-able, 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.**

- 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 requires the existence of:
  - an information collection site, such as a Web page or portal, where governance information is stored and from which the information is always available for access;
  - a mechanism to inform **participants of significant governance events,** such as changes in policies, rules, or regulations;
  - accessible storage of the specifics of Governance Processes;
  - SOA services to access automated implementations of the Governance Processes:

- Governance policies are made operational through rules and regulations. This requires the existence of:
  - descriptions to enable the rules and regulations to be visible, where the description includes a unique identifier and a sufficient, and preferably a machine process-able, 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 automated implementations of the Governance Processes.

Architectural Implications of SOA Security

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

- Security expressed through policies have the same architectural implications as described in Section for policies and contracts architectural implications.
- 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.

- The mechanisms that make-up the execution context in secure SOA-based systems should:
  - provide protection of the confidentiality and integrity of message exchanges;
  - be distributed so as to provide centralized or decentralized policy-based identification, authentication, and authorization;
  - ensure service availability to consumers;
  - be able to scale to support security for a growing ecosystem of services;
  - be able to support security between different communication technologies;
- Common 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.

Conclusions

- As ontology provides the representation of a choosen architecture, the architectural principles have direct impact on the definition of ontologies.
- The SOA architectures comply with the recently provided and currently developed security and privacy related HL7 artifacts.
- Differences result from not considering granularity levels and domain specifities, which are represented by the GCM.
- The GCM enables to related and to bridge between the specifications.
- Academic teams from different universities currently work on the model mapping needed.