Chapter 3

Elements identified for the Framework

This chapter explains the different elements/entities identified and defined in this work in order to understand the security policy framework. The security policy framework and its authentication, privacy, trust and authorization models are based on these elements. Following are the major elements/entities of the framework.

Subject (SU): Subject is an entity that wants to access services/resources. It can be a user, a service or any other entity on behalf of user/service.

Service (SR): Service is a piece of software that provides some functionality and can be accessed by Subjects or other Services. Services are exposed in the environment along with their associated Service Policies and are found by Subjects. Services are provided by different Service Providers.

Resource (R): Resource is a sharable object that can be accessed by Subjects. It can be a CPU, a storage device, software, data, scientific instrument or any other peripheral. Subjects access Resources through Services. In other words, a Resource provides a Service. Subjects can access Resources based on their authorization status and their conformance to established authentication, privacy, trust, authorization and other security policies. There are two types of resources:

i) Subject's Resources: These are the resources which are provided by Subjects to Service Providers. *e.g.* Subject's name, date of birth, his private telephone number *etc.*

ii) Service Provider's Resources: These are the resources which are provided by Service Providers to Subjects. Subjects can access these Resources based on their authorization status and their conformance to established security policies.

Service Policy (SrP): Service Policy refers to the set of rules/requirements associated with a Service. A Subject must conform to Service Policy in order to access that Service.

Domain (DO): Domain refers to the set of Subjects, Services and Service Providers under a unique Domain Policy (DP). The Services in a Domain are provided by Service Providers and they may belong to same or different physical organizations/institutions.

Domain Policy (DP): Domain Policy refers to the set of rules/regulations/requirements of a Domain, which a Subject must satisfy in order to access the Services/Resources provided by that Domain.

Service Provider (SP): The term Service Providers refers to physical organizations/ institutions that provide Services/Resources in a Domain. A Service Provider can provide Services/Resources in any number of Domains. Services/Resources in a Domain may come from same or different Service Providers. Thus a Domain is a more dynamic entity than individual physical organization/institution.

Service Provider Policy (SPP): The Service Provider Policy refers to the set of rules/regulations/requirements of a Service Provider, which a Subject must satisfy in order to access the Services/Resources provided by that Service Provider.

Access (AC): Access is an operation or set of operations that a Subject performs on a Service/Resource. The access is provided based on conformance to Service Policy (SrP) and other applicable security policies that are associated with that Service/Resource or the access request.

Filter (FL): The rights/privileges of a Subject are different in different Domains. Filter is a component through which rights/privileges of a Subject are attenuated / filtered for a particular Domain. There are two types of Filters: Filter-In (FL-I) and Filter-Out (FL-O). Through Filter-Out component, the Subject leaves the Domain with access rights that his Domain grants to him. Through Filter-In component, the Subject enters the target Domain with access rights that the target Domain grants to Subject's Domain. These will be explained in detail later in this section.

Policy (PO): Policy is a set of rules/requirements that can be associated with Subject/Service/Service Provider/Domain *etc*. Policies can be of different types. Policy can be represented as set PO = {ANP, PP, TP, AP, OP} where

ANP is Authentication Policy

PP is Privacy Policy

TP is Trust Policy

AP is Authorization Policy

and OP refers to any Other Policy

These policies deal with issues specific to authentication, privacy, trust, authorization and other aspects and will be defined and explained in Chapter 4. Service Policy (SrP), Service Provider Policy (SPP) and Domain Policy (DP) are subsets of Policy (PO). *i.e.* SrP $\subseteq$ PO, SPP $\subseteq$ PO and DP $\subseteq$ PO.

Privacy Index (PI): Privacy Index indicates the privacy level of Subject's Resources. Subject's Resources are marked with a PI value. Higher values of PI mean more privacy. Private data/information is marked with higher values of PI. PI can take following values:

PI Value	Privacy Level	Meaning
0	No Privacy	Subject's Resource can be used anyway.
1	Partial Privacy	Subject's Resource can be used with permission only.
2	Time Limited Privacy	Subject's Resource can be used with permission but for a limited time period.
3	Full Privacy	Subject's Resource can not be used under any circumstances.

Table 3.1: Privacy Index levels and their meaning

Purpose (PU): Purpose element tells the purpose for which Subject's Resources (*e.g.* his private/public information) are required by Service Providers. A Service Provider may require Subject's Resources for research / marketing / data mining / to provide customized access to Services *etc.*

Action (ACT): Action element tells what operations/actions can be performed on i) Subject's Resources by Service Providers and ii) Service Providers' Resources by Subjects. These operations/actions can be read/ write/ execute/ copy/ share/ distribute/ update/ delete/ append/ view *etc.* Exact operation depends on the resource under consideration. Different types of Resources support different types of operations/actions on themselves.

Conditions (CO): Conditions are privacy statements which describe some prerequisites that must be satisfied before granting access to Resources/Services. *e.g.* a Condition may state that Subject's age must be greater than 18 in order to access a Service/Resource. Though Conditions can be specified through policy associated with that Service/Resource but specifying privacy statements separately for a Service/Resource enable us to implement privacy based access control in a more meaningful and efficient way. This will be explained later in the Privacy Model.

Obligations (OB): Obligations are activities that must be performed by Service Providers while providing access to Resources/Services or while accessing Subjects Resources. Example of obligation can be to send a notification e-mail to parents if their children access a particular Service.

Consent (C): Consent is the permission given by Subjects/Service Providers, who provide their Resources, to explicitly state that their Resources/Services can be used for a particular Purpose. *e.g.* a Subject may explicitly state that his telephone number can be used by marketing people to inform him about new schemes.

Authority (A): Authority is an administrative entity that is capable and authoritative of issuing, validating and revoking an electronic means of proof. Authority can be classified as i) Identity Authority ii) Authorization Authority and iii) Attribute Authority

i) Identity Authority: Identity Authorities make assertions about the identity of the Subject. Certificate Authorities (CAs) are examples of Identity Authorities.

ii) Authorization Authority: Authorization Authorities make assertions about the authorization rights of a Subject. In the implemented framework, Filter components make authorization assertions. Identity Authorities enable authentication whereas Authorization Authorities enable authorization.

iii) Attribute Authority: Attribute Authorities issue attribute assertions that a given Subject has one or more attribute/value pair.

Privacy Controller (PC): is an entity that checks misuse of Subject’s Resources at Service Provider’s end *i.e.* it works for Subjects interests. It makes sure for Subjects that Service Providers are respecting Subject’s privacy requirements and are accessing/ providing access to Subject’s Resources only for the purpose for which they have been sent.

Trusted Third Party (TTP): is an independent entity that is trusted by both, the Service Requesters (Subjects) and Service Providers. Subjects can use it to obtain signed credentials which they can later provide to Service Providers to obtain access (including anonymous access) to their Resources/Services. Service Providers can make use of TTP to hide Service details from Subjects. TTP plays an important role in handling Service Provider’s and Service Requester’s privacy requirements. TTP can be run by a government agency in order to make Service Providers and requesters to trust it. PC can also be a part of TTP.

MAP (MAP): is an operation that maps/transforms Subject of one administrative domain to Subject in another administrative domain. *e.g.* SU_i (DO_k) → map→ SU_j (DO_l) means that Subject SU_i of Domain DO_k has been mapped to Subject SU_j in Domain DO_l.

Grid Elements Set (GES): refers to the set GES = {SU, SR, R, SP, DO, A, PC, TTP} *i.e.* the set of entities that interact with each other in a grid environment.

Grid Environment (GE): refers to the distributed environment in which different entities of Domain or sets of different Domains interact with each other.

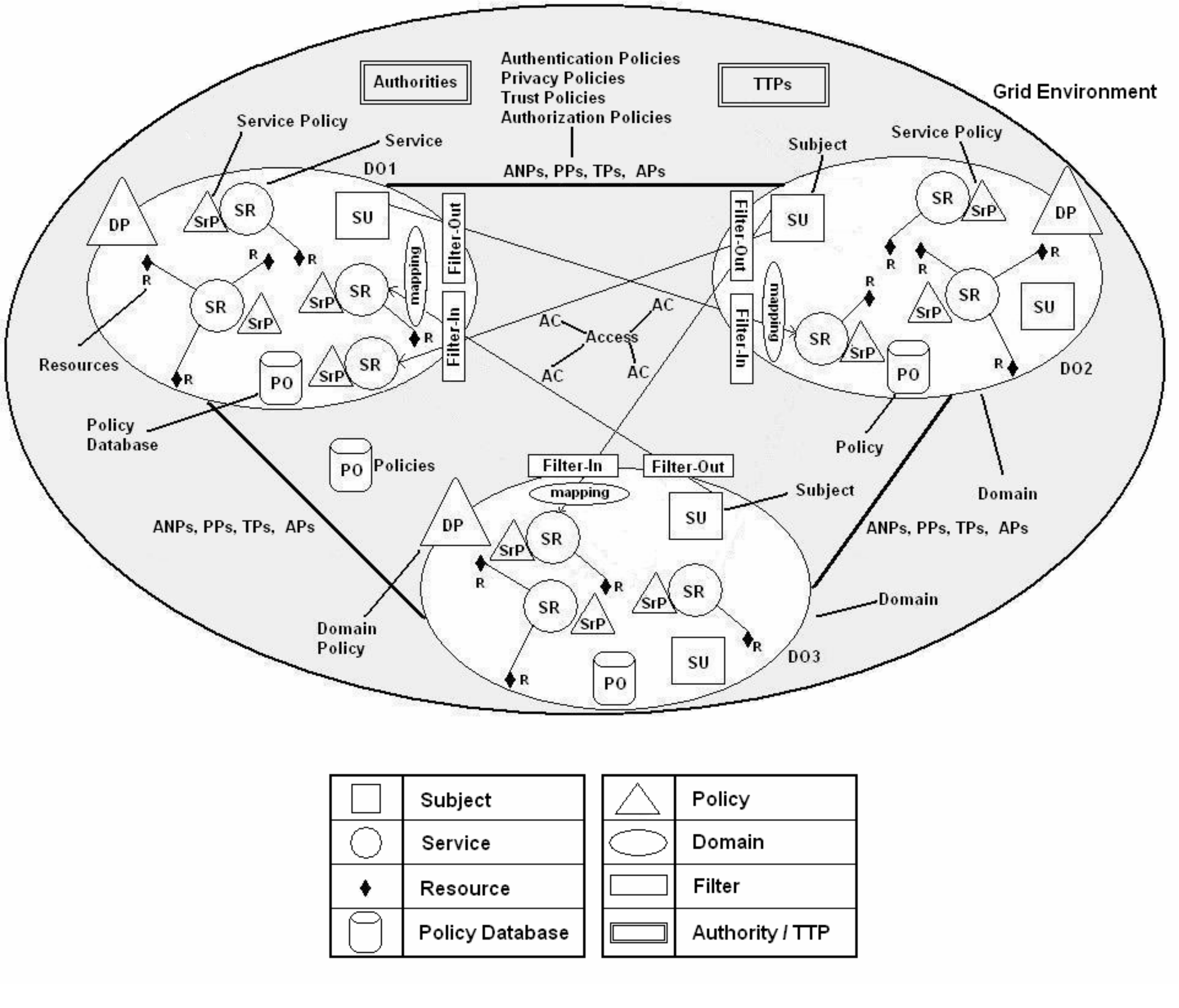

Figure 3.1: Schematic showing Grid Environment consisting of three domains along with other elements of the security framework

In a typical Grid Environment, the grid entities described above interact in a complex manner. The secure access of Services/Resources among different entities in such an environment demands a security framework. The focus of the thesis is to implement such a framework.

Figure 3.1 represents a blueprint of the envisioned Grid Environment. It consists of three Domains (DO1, DO2 and DO3) along with other elements of the security framework. In the diagram squares represent Subjects, circles represent Services, diamonds represent Resources, triangles represent Policies, rectangles represent Filters and ellipses represent Domains. As shown in Figure 3.1, Subject's access request for Service SR first passes through Filter-Out component at the source Domain and then through Filter-In component at the target Domain. During this passage, Subject's access rights are filtered for the target Domain. Through Filter-Out component, the Subject leaves the Domain with access rights that his parent Domain grants to him and through Filter-In component, the Subject enters the target Domain with access rights that the target Domain grants to Subject's parent Domain. In other words, the Subject gets the intersection of the rights that his parent Domain grants to him and the rights that target Domain grants to Subject's parent Domain. Filter components make the authorization system scalable and flexible.

To understand the use of Filter-In and Filter-Out components consider that a Domain, say Domain-A, has 100 subjects who perform either "read", "update" or "execute" operations on a file through Service SR-1 provided by Domain-B. As the number of subjects accessing the Service SR-1 is large, it will be difficult for Domain-B to maintain access rights information of each and every subject of Domain-A, for SR-1. So here Domain-B will store the information that any of the subjects from Domain-A can perform read, update and execute operation on file through SR-1, but, the more fine grained access rights information *i.e.* which subjects of Domain-A can perform which actions on that file through SR-1, will be maintained by Domain-A itself. This concept will make the authorization system flexible and scalable. This concept has been implemented in the framework through Filter-Out and Filter-In components. In this particular example, Filter-Out component will store access rights information regarding which subjects of Domain-A can perform which actions on SR-1 and Filter-In component will store access rights information regarding the actions that can be performed on SR-1 by the subjects of Domain-A.

Now consider that Domain-A allows one of its subjects, say SU-1, to perform "read" and "update" operations on the file through SR-1. If SU-1 tries to perform "execute" operation on the same file then Filter-Out component will not allow this request to pass through it as it has information regarding which subject can perform which action on file. As SU-1 is not allowed by Domain-A to perform "execute" operation on file, Filter-Out component will restrict this access request. On the other side, if Domain-A allows one of its subjects to perform "delete" operation (intentionally or unintentionally) on the same file then Filter-In component of Domain-B will not allow this request to pass through it as it has information regarding the actions that can be performed on SR-1 by the subjects of Domain-A. As Domain-B does not allow any of the subjects of Domain-A to perform "delete" operation on the file, Filter-In component will restrict this request. Filter components are making the authorization system scalable *e.g.* in this case, subject wise access rights information is being maintained by Domain-A through Filter-Out component and domain wide access rights information is being maintained by Domain-B through Filter-In component. A single Domain is not maintaining all the access rights information. Thus the authorization system is scalable.

The mapping operation (MAP) is performed to provide the Subject an identity that is local to the target Domain. The mapped identity is used by the target Domain to provide access to the requested Service/Resource. The mapping operation is optional. It is performed only if access of a Service/Resource explicitly requires local identity. If the access of a Service/Resource does not require local identity then MAP is not performed. The role of other elements like Privacy Index, Purpose, Privacy Controller etc. will be explained in Chapter 5 while explaining Privacy Model as these elements play major role in providing privacy based access to grid services.

Figure 3.1 also shows Policy database to store different types of policies. Domains can have different authentication, privacy, trust and authorization related requirements and policies among each other. These policies can also exist among Subjects and Services of different Domains in a complex manner. Determining whether a Subject conforms to all applicable policies is a complex task. In the implemented framework, it is performed by Authorization Handler with the help of other components like Privacy Handler, Trust Handler etc. At the target Domain, the integrated policy based authorization framework checks Subject's conformance to Domain Policy (DP), Service Provider Policy (SPP), Service Policy (SrP) and other applicable policies. If Subject does not conform to any of these policies, the access is denied.

The detailed architecture and explanation of the implemented framework is given in Chapter 5. Next chapter describes different types of security policies that have been identified, categorized and focused in the framework. The chapter also describes how these policies have been expressed and exposed in the environment.