Design and Implementation of a Framework for Assured Information Sharing Across Organizational Boundaries

Bhavani Thuraisingham, The University of Texas at Dallas, USA
Yashaswini Harsha Kumar, The University of Texas at Dallas, USA
Latifur Khan, The University of Texas at Dallas, USA

ABSTRACT

In this article we have designed and developed a framework for sharing data in an assured manner in case of emergencies. We focus especially on a need to share environment. It is often required to divulge information when an emergency is flagged and then take necessary steps to handle the consequences of divulging information. This procedure involves the application of a wide range of policies to determine how much information can be divulges in case of an emergency depending on how trustworthy the requester of the information is.

Keywords: Assured Information Sharing (AIS); XACML

INTRODUCTION

Organizations including healthcare, military, and financial have to form coalitions and collaborate to solve a particular problem such as the global war on terror or provide joint services to customers. However each organization of a coalition has to enforce policies to ensure that information is shared in a secure manner. This concept as come to be known as assured information sharing (AIS). In our previous article we have described our approach to AIS. Our work was initially based on a need to know paradigm where the organizations share data according to the policies. However in many situations information has to be divulged in case of emergencies. For example, in a high security building, the building plan is not easily accessible and distributable information. But in case of an emergency such as an evacuation in case of fire, people normally unauthorized to such information are permitted to access it. For example consider a case of fire where some
employees may be trapped and the building maintenance personnel are unavailable to help out. But using devices that may be able to fetch data, they may be able to use exit routes.

The work described in this article discusses the design and implementation of a XML-based framework for a need to share environment. In particular, we have designed and developed a Trusted Computing Base (TCB) which is essentially our framework for Assured Information Sharing that deals with the “need-to-share” paradigm. This paradigm shift is one of the recommendations of the 9/11 commission. This deals with dynamic environments with better flow of information. A Trusted Computing base creates a hierarchy for users of the system based on how trustworthy a user is. The level of trust can be as fine grained as possible. Based on the trust level and severity of the emergency, information is disseminated to the user.

The organization of our article is as follows. In the Assured Information Sharing section we provide some challenges in assured information sharing including aspects of policy enforcement. The design and implementation of our prototype framework is discussed in the Design and Implementation of the Framework section. The article is concluded in the Summary and Directions section. The appendix consists of a set of policies that we have defined for our environment.

**ASSURED INFORMATION SHARING**

A coalition consists of a set of organizations, which may be agencies, universities and corporations that work together in a peer-to-peer environment to solve problems such as intelligence and military operations as well as healthcare operations. Figure 1 illustrates our architecture for a coalition where three agencies have to share data and information. Coalitions are usually dynamic in nature. That is, members may join and leave the coalitions

---

**Figure 1. Architecture for organizational data sharing**

![Architecture for organizational data sharing](image)

---

Copyright © 2008, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
in accordance with the policies and procedures. A challenge is to ensure the secure operation of a coalition. We assume that the members of a coalition, which are also called its partners, may be trustworthy, untrustworthy or partially (semi) trustworthy.

Security policies include policies for confidentiality, privacy, trust, release, dissemination and integrity. A broader term is dependable systems or trustworthy systems that also include real-time processing and fault tolerance. We will discuss dependability in the next section. By confidentiality we mean that data is only released to individuals who are authorized to get the data. Privacy in general deals with the situation where an individual determines what information should be released about him/her. (Note that different definitions of privacy have been proposed.) Trust policies may add further restriction to privacy and confidentiality policies. For example, a user may be authorized to get the data according to the confidentiality policies, but the system may not trust the individual in which case the data is not released. Similarly a person may give permission to release certain private information about him or her but that person may not trust a particular web site in which case the private information is not released to the web site. Alternatively one could argue that one needs to establish trust first before establishing the confidentiality and privacy policies. For example, a user’s (or web site’s) trust is established before determining that the user (or web site) can received confidential (or private) information. Release policies specify rules for releasing data while dissemination policies specify rules for disseminating the data. Integrity within the context of security ensures that only authorized individuals can modify the data so that the data is not maliciously corrupted.

There is a critical need for organizations to share data as well process the data in a timely manner, but at the same time enforce various security policies. For example, A and B form a coalition while B and C form a second coalition. A could be California, B could be Texas and C could be Oklahoma. California and Texas could form a coalition as part of the larger states in the US and Texas and Oklahoma could form a coalition as part of the neighboring states in the South of US for emergency management. There is also an urgent need for multiple organizations to share data and at the same time enforce security policies. These policies include policies for confidentiality, privacy, and trust. For example, patient data may be shared by multiple organizations including hospitals, levels of government and agencies. It is important to maintain the privacy of patient data. However it is also important that there are no unnecessary access controls so that information sharing is prohibited. One needs flexible policies so that during emergency situations it is critical that all of the data is shared so that effective decisions can be made. During normal operations, it is important to maintain confidentiality and privacy. In addition, trust policies ensure that data is shared between trusted individuals.

DESIGN AND IMPLEMENTATION OF THE FRAMEWORK

Background
In this section, we will provide some background information including our route finder application, an example as well as some basics in XACML, which is the XML Access Control specification produced by the OASIS standards organization.

Route Finder Application
The application that has been developed is used to demonstrate the concept of TCB is Route Finder. This application is used to find routes between two locations. This application has two parts:

1. Normal Case
2. Emergency Case The application considers some routes to be top secret. Policies are used to specify the conditions in which routes using these locations can be
accessed. For example top level Government employees have access to the widest range of locations/route information. A few policies have been integrated into the implementation and many others are specified using XACML policies.

**Example:** Consider a situation where a top level government employee has to access some route information involving the location of a private entity. He can do so based on the level of emergency. Access based on emergency is logged so that this information is available for handling the consequences. This involves a certain level of access control implemented through username and password. The Route-Finder application can be accessed anonymously too, in which case the emergency case feature is disabled.

**XACML** XACML is an OASIS standard that describes both a policy language and an access control decision request/response language (both encoded in XML) [5]. Using XACML, one can specify access control policies. These policies can be grouped into Policy sets. Based on these policies, it is possible to determine whether a particular access request can be fulfilled. XACML returns the answer to the policy request as one of the four possible values: Permit, Deny, Indeterminate or Not Applicable. XACML specifies two entities: The Policy Enforcement Point (PEP) and the Policy Decision Point (PDP). The PDP returns the answer to a request passed by the PDP in one of the following answer values: Permit, Deny, Intermediate or Not Applicable. This decision is made based on the access control policy specified in the XACML policy files. Though the PDP makes the decision regarding a request, the PEP is responsible for enforcing the decision to grant/deny access.

Policy Files specify rules for “Targets”. Each target is composed of three components: Subject, Resource and Action; each target is identified uniquely by its components taken together. The XACML request generated by the PEP contains the target. The PDP’s decision-making capability lies in matching the target in the request file with the target in the policy file.

**Design of the Framework**

The aim of our project is to build a system capable of serving emergency requests on a need-to-share basis. The Route-Finder application serves web-based requests. It categorizes the users of the system into a hierarchy in which users at each level have a different level of trust. The users in the topmost layer are the most trusted.

- **The Trusted Computing Base:** The trusted computing base is the wrapper around the Assured Information sharing portal for information dissemination on a need-to-know basis. This wrapper handles the dissemination of information on a need-to-share basis. It contains policies to support emergency requests. The Route Finder application operates in two modes: Normal: In this mode, the information is disseminated based on normal access control method of username-password. No information related to secret locations is disseminated. An anonymous user can also use the Route Finder application in the normal mode. Secret locations do not appear on the map. Emergency: In this mode, authenticated users can issue requests to obtain route information involving secret locations based on certain policies. For example top government officials have access to many secretive locations. At the same time, the access to such information is also dependent on the level of severity. These operations are logged so that actions can be taken for dealing with the consequences of disseminating confidential information.

- **Database:** The information about routes is stored in database. This database also contains user information for authentication. The route and user information obtained in the databases can be obtained by executing SQL queries. The relational schemas present in the database are as follows:
• **Schemas:** We describe the schemas that we have designed for the database.

**CITY**

<table>
<thead>
<tr>
<th>Name</th>
<th>Id</th>
<th>Private</th>
</tr>
</thead>
</table>

This schema is used to depict a location. The “Private” field specifies whether this location is a secret location or not.

**CITY LOC**

<table>
<thead>
<tr>
<th>Cid</th>
<th>X</th>
<th>Y</th>
</tr>
</thead>
</table>

This schema describes the position of the city or location in terms of X and Y coordinates.

**DIVISION**

<table>
<thead>
<tr>
<th>Name</th>
<th>DId</th>
<th>Priority</th>
</tr>
</thead>
</table>

This schema is used to describe a level in the hierarchy. Users belonging to a particular division belong to a level in the hierarchy.

**ROUTE**

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Path</th>
<th>Private</th>
</tr>
</thead>
</table>

This schema provides the path information for a different source-destination pairs. Private routes are not available in the normal mode of execution.

**USER**

<table>
<thead>
<tr>
<th>Name</th>
<th>Id</th>
<th>Uname</th>
<th>Pwd</th>
<th>DId</th>
</tr>
</thead>
</table>

This schema provides user information for authentication and for determining privileges.

• **Policy Files:** Each location has a privacy file specifying the access for users in different divisions or levels. Different policies also exist for different users at different severity levels. These policy files can be derived from the trust level of each level of users.

The architecture of the Route finder application is as shown in Figure 2. The Confidential information refers to the Route and location information. The Response Engine refers to the XACML PEP-PDP.

• **Response Engine:** Serves queries passed down from the TCB. This engine translates web interface/web service queries to XACML requests. It also converts the XACML response to a format compliant with the web service/web interface. The Response Engine contains two sub-components: **Policy Enforcement Point** and the **Policy Decision Point**.

- **Policy Enforcement Point (PEP):**
  - Enforces policies on requests sent by the Web Service.
  - Translates this request into an XACML request; sends it to the PDP.

- **Policy Decision Point (PDP):**
  - Makes decisions regarding the request made by the web service.
  - Conveys the XACML request to the PEP.

**Implementation of the Framework**

The implementation of the Route-Finder Application has been done in Java using the NetBeans IDE 5.5®. The front end is web based with Java Servlet Pages. The backend consists of a MySQL® database named as TCB and the connection to the database is through JDBC. The business logic is applied thought the use of XACML policies and some integrated into the implementation. The XACML policy files can dynamically change. A policy file exists for each private location containing rules for access in case of emergency situations based on the level of severity. The output (route) of the Route Finder application is a .jpg file pictorially depicting the route obtained. The routes may vary for emergency and normal route situations. If new private locations are added, it is necessary to specify a policy file mentioning the access rules for various levels of severity.
The NetBeans IDE® deploys the Tomcat Server. The JSPs, Servlets and XACML policies are all integrated into the NetBeans IDE®.

I. Main screen: This page (illustrated in Figure 3) is accessible to all and is the main page for all users. Any user can anonymously use the system with username “Anonymous” and blank password for limited capabilities. Other users are authenticated based on the username and password that is entered.

II. Normal Mode Execution Screen: Figure 4 illustrates the normal model screen. This mode is accessible by all users. For Anonymous users, the link for ‘Emergency Execution mode” does not exists. Secret locations cannot be obtained through the normal execution mode.

III. Normal Execution Route (A -> D): Figure 5 illustrates the normal execution route. The output of normal execution is a .jpg file. The request for normal execution route from Source A to destination D yielded the above route.

IV. Emergency mode Execution Screen: Figure 6 illustrates the emergency mode execution screen. This screen is used for emergency situations and the user is allowed to choose private locations and routes to private locations or those involving them and also the severity to indicate the severity of the emergency. If no special routes are found, the user is directed to the normal execution mode screen.

V. Emergency Execution Route (A->D): Figure 7 illustrated the emergency execution route; the output of emergency execution is a .jpg file. The request for emergency execution route from Source A to destination D yielded the above route.

The emergency case execution details are logged into a log file. The details include the username, severity level, source and the destinations cities/locations.

Sample Log File Contents

<table>
<thead>
<tr>
<th>garnet#3#A#D</th>
<th>pepper#3#A#UTD</th>
<th>eutd#1#A#UTD</th>
</tr>
</thead>
<tbody>
<tr>
<td>eutd#3#A#LNT</td>
<td></td>
<td>garnet#3#A#D</td>
</tr>
</tbody>
</table>
Sample Rule for an Employee of Division Gov1 to Access a Location “LNT” when the Severity Level is 3

```xml
<Rule
    RuleId="Emergency:Gov1:3"
    Effect="Permit">
    <Description>
      Government 1 agencies can access this location at severity level 3.
    </Description>
    <Target>
      <Subjects>
        <Subject>
          <SubjectMatch
              MatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal">
            <AttributeValue
                DataType="http://www.w3.org/2001/XMLSchema#anyURI">
              http://Route-Finder.com/emergency/Level-3/GOV1</AttributeValue>
            <SubjectAttributeDesignator
                AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
                DataType="http://www.w3.org/2001/XMLSchema#anyURI"/>
          </SubjectMatch>
        </Subject>
      </Subjects>
      <Resources>
        <Resource>
          <ResourceMatch
              MatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal">
            <AttributeValue
                DataType="http://www.w3.org/2001/XMLSchema#anyURI">
              http://Route-Finder/CityUTD</AttributeValue>
            <ResourceAttributeDesignator
                AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
                DataType="http://www.w3.org/2001/XMLSchema#anyURI"/>
          </ResourceMatch>
        </Resource>
      </Resources>
      <Actions>
        <Action>
          <ActionMatch
              MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue
                DataType="http://www.w3.org/2001/XMLSchema#string">
              access-route</AttributeValue>
            <ActionAttributeDesignator
                AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
                DataType="http://www.w3.org/2001/XMLSchema#string"/>
          </ActionMatch>
        </Action>
      </Actions>
    </Target>
</Rule>
```
Figure 3. Main screen

Figure 4. Normal mode execution screen
Figure 5. Normal Execution Route (A -> D)

Figure 6. Emergency Mode execution Screen
• **Setting up the database:** This project makes use of a MySQL database called “TCB”. This database is stored in the “Databases” folder. They are all needed for the proper execution of the project. Once MySQL® is installed,
  1. Open the DOS command prompt.
  2. Change to the “Databases” directory.
  3. Execute the following commands:
  4. Start MySQL® by executing the command: `mysql`.

• **Running the project:**
  1. Open the NetBeans® IDE.
  2. Click on “Open Project” in the “File” menu.
  3. Browse for the directory “TCB” in the “Source” directory. Once NetBeans® is installed, all project folders are uniquely identified by an icon superimposed on the folder.
  4. Open the TCB project.
  5. Click on “clean and Build Main Project” in the “Build” menu.
  6. Click on “Run Main Project” in the “Run” menu.
  7. A browser opens up with the

• **Contents of the Database:**
  - **Division:** Currently, 7 divisions exist: GOV1, GOV2, GOV3, UTD, LNT, IMB and XXX for Anonymous. **User:** The database includes one user for each of the divisions: GOV1, GOV2, GOV3, UTD and LNT. Take a look at the databases for username/password. **City:** The city/location currently existing in the database includes: A, B, C, D, UTD and LNT. UTD and LNT are private locations. **Route:** Currently only some select routes exist. The routes table can be expanded to include more routes.
  
• **Policy Files:** Policy Files exist for the private locations: UTD and LNT are named CityUTD.xml and CityLNT.xml respectively.

• **Request Files:** Request Files exist for each division to access the private locations.

**SUMMARY AND DIRECTIONS**
The Trusted Computing Base deals with disseminating information in case of emergencies. The policy of TCB is to disseminate information and then deal with the consequences by auditing, and so forth. This project has been highly
influenced by the 9/11 Commission Report Recommendations. The world now recognizes the importance of “need-to-share” information to fight terrorism. Need to share information is also important in cases of medical emergencies and natural calamities.

The next main step would be to integrate this project with the ArcGIS® framework to extend it to various maps. This would involve enriching the dataset that currently exists to include more locations and routes. This would involve considerable effort by persons trained with the ArcGIS® tools. ArcGIS is geospatial and mapping software used to perform spatial analysis, manage large amounts of spatial data and produce maps to aid decision making.

Next would be implementing the interface for web service agents. This would involve exporting an API for webs service agents. This API would allow requests to be sent to the TCB. Web service agents belonging to various organizations can query the TCB without a user having to manually input the query as is the case now. The authentication and authorization mechanisms can work on the identification sent by these agents instead of the current username/password method. This allows the coalition system to be scalable as it can allow for various means of authorization/authentication; for example, through the use of certificates.

Currently, the requests are hard-coded in the application as request files. This method is not scalable. As the number of divisions and private locations increase in the databases, creating a request file for each access operation manually will be tedious and unmanageable. The request files can be created on-the-fly using APIs provided by Sun’s implementation of XACML; it can be included as part of the PEP’s business logic.

Policies can be made more granular. This could be done by adding more rules in the policy files or by determining different levels of execution in the implementation. Implementation based could be more to do with the need-to-know paradigm and the policy files based decisions could be more need-to share paradigm based.

Auditing of logged data: It is necessary to audit the data that has been logged to monitor possible security breaches. The data is logged into a text file. It is necessary to apply an auditing process to check whether the data that has been disseminated is being used efficiently and that the emergency does really exist with that severity level.

The application can be enhanced to use real location information and depict the locations and routes on a map using the Google Maps® API.

ACKNOWLEDGMENT

The research reported in this article was partially funded by grants from the Air Force Office of Scientific Research and from the National Science Foundation under the Cyber Trust program.

REFERENCES


APPENDIX

Policy File for Location UTD:

```xml
<?xml version="1.0" encoding="UTF-8"?>
<!--Document : CityUTD.xmlCreated on : November 13, 2007, 9:30 AMAuthor : yxh068000Description: Purpose of the document follows.-->
  <Description>This policy file specifies the rules to be evaluated for a user accessing the locationUTD based on the division the user belongs to and the severity of the emergency. </Description>
  <Target>
    <Subjects>
      <AnySubject/>
    </Subjects>
    <Resources>
      <AnyResource/>
    </Resources>
    <Actions>
      <AnyAction/>
    </Actions>
  </Target>
  <Rule RuleId="Emergency:Gov1:3" Effect="Permit">
    <Description>
    </Description>
  </Rule>
</Document>
```
Government 1 agencies can access this location at severity level 3.

<Description>
<Target>
<Subjects>
<Subject>
<SubjectMatchMatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal"><AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#anyURI">http://Route-Finder.com/emergency/Level-3/GOV1</AttributeValue>
<SubjectAttributeDesignatorAttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"DataType="http://www.w3.org/2001/XMLSchema#anyURI"/>
</SubjectMatch>
</Subject>
</Subjects>
<Resources>
<Resource>
<ResourceMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal"><AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#anyURI">http://Route-Finder/CityUTD</AttributeValue>
<ResourceAttributeDesignatorAttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"DataType="http://www.w3.org/2001/XMLSchema#anyURI"/>
</ResourceMatch>
</Resource>
</Resources>
<Actions>
<Action>
<ActionMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal"><AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">access-route</AttributeValue>
<ActionAttributeDesignatorAttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"DataType="http://www.w3.org/2001/XMLSchema#string"/>
</ActionMatch>
</Action>
</Actions>
</Target>
</Rule>

<Rule
RuleId="Emergency:Gov1:2"
Effect="Permit">
<Description>
Government 1 agencies can access this location at severity level 2. </Description>
</Rule>
<Subjects>
<Subject>
<SubjectMatchMatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal"><AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#anyURI">http://Route-Finder.com/emergency/Level-2/Gov2</AttributeValue>
<SubjectAttributeDesignatorAttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"DataType="http://www.w3.org/2001/XMLSchema#anyURI"/>
</SubjectMatch>
</Subject>
</Subjects>
</Rule>
Government 2 agencies can access this location at severity level 3.

</Description>
</Target>
</Subjects>
</Subject>
</Resources>
</Resource>
</Actions>
</Action>
</Target>
</Rule>

15
<ResourceMatch>
</Resource>
</Resources>
<Actions>

<Action>
<ActionMatch>
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal"><AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">access-route</AttributeValue>
<ActionAttributeDesignatorAttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
DataType="http://www.w3.org/2001/XMLSchema#string"/>
</ActionMatch>
</Action>
</Actions>
</Target>
</Rule>

RuleId="Emergency:Gov3:3"
Effect="Permit">

<Description>
Government 3 agencies can access this location at severity level 3.</Description><Target>

<Subjects>

<SubjectMatchMatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal"><AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#anyURI">http://Route-Finder.com/emergency/Level-3/GOV3</AttributeValue>
<SubjectAttributeDesignatorAttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"DataType="http://www.w3.org/2001/XMLSchema#anyURI"/>
</SubjectMatch>
</Subject>
</Subjects>

<Resources>

<Resource>
<ResourceMatch>
MatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal"><AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#anyURI">http://Route-Finder/CityUTD</AttributeValue>
<ResourceAttributeDesignatorAttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"DataType="http://www.w3.org/2001/XMLSchema#anyURI"/>
</ResourceMatch>
</Resource>
</Resources>

<Actions>

<Action>
<ActionMatch>
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal"><AttributeValue
Data......
<Rule RuleId="Emergency:Utd:3" Effect="Permit">
  <Description>
    Users belonging to the UTD division can access this location at Severity level 3.
  </Description>
  <Target>
    <Subjects>
      <Subject>
        <SubjectMatchMatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal"><AttributeValue
            DataType="http://www.w3.org/2001/XMLSchema#anyURI">http://Route-Finder.com/emergency/Level-3/UTD</AttributeValue>
          <SubjectAttributeDesignatorAttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id" DataType="http://www.w3.org/2001/XMLSchema#anyURI"/>
        </SubjectMatch>
      </Subject>
    </Subjects>
    <Resources>
      <Resource>
        <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal"><AttributeValue
            DataType="http://www.w3.org/2001/XMLSchema#anyURI">http://Route-Finder/CityUTD</AttributeValue>
          <ResourceAttributeDesignatorAttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id" DataType="http://www.w3.org/2001/XMLSchema#anyURI"/>
        </ResourceMatch>
      </Resource>
    </Resources>
    <Actions>
      <Action>
        <ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal"><AttributeValue
            DataType="http://www.w3.org/2001/XMLSchema#string">access-route</AttributeValue>
          <ActionAttributeDesignatorAttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id" DataType="http://www.w3.org/2001/XMLSchema#string"/>
        </ActionMatch>
      </Action>
    </Actions>
  </Target>
</Rule>
<Rule RuleId="Emergency:Utd:2" Effect="Permit">
  <Description>
    Users belonging to the UTD division can access this location at Severity level 2.</Description>
  <Target>
    <Subjects>
      <Subject>
        <SubjectMatchMatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal"><AttributeValue
          DataType="http://www.w3.org/2001/XMLSchema#anyURI">http://Route-Finder.com/emergency/Level-2/UTD</AttributeValue>
        <SubjectAttributeDesignatorAttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"DataType="http://www.w3.org/2001/XMLSchema#anyURI/>
      </Subject>
    </Subjects>
    <Resources>
      <Resource>
        <ResourceMatchMatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal"><AttributeValue
          DataType="http://www.w3.org/2001/XMLSchema#anyURI">http://Route-Finder/CityUTD</AttributeValue>
        <ResourceAttributeDesignatorAttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id" DataType="http://www.w3.org/2001/XMLSchema#anyURI/>
      </Resource>
    </Resources>
    <Actions>
      <Action>
        <ActionMatchMatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal"><AttributeValue
          DataType="http://www.w3.org/2001/XMLSchema#string">access-route</AttributeValue>
        <ActionAttributeDesignatorAttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id" DataType="http://www.w3.org/2001/XMLSchema#string"/>
      </ActionMatch>
    </Actions>
  </Target>
</Rule>

<Rule RuleId="Emergency:Utd:1" Effect="Permit">
  <Description>
    Users belonging to the UTD division can access this location at Severity level 1.</Description>
  <Target>
    <Subjects>
      <Subject>
        <SubjectMatchMatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal"><AttributeValue
          DataType="http://www.w3.org/2001/XMLSchema#anyURI">http://Route-Finder.com/emergency/Level-1/UTD</AttributeValue>
        <SubjectAttributeDesignatorAttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"DataType="http://www.w3.org/2001/XMLSchema#anyURI/>
      </Subject>
    </Subjects>
    <Resources>
      <Resource>
        <ResourceMatchMatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal"><AttributeValue
          DataType="http://www.w3.org/2001/XMLSchema#anyURI">http://Route-Finder/CityUTD</AttributeValue>
        <ResourceAttributeDesignatorAttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id" DataType="http://www.w3.org/2001/XMLSchema#anyURI/>
      </Resource>
    </Resources>
    <Actions>
      <Action>
        <ActionMatchMatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal"><AttributeValue
          DataType="http://www.w3.org/2001/XMLSchema#string">access-route</AttributeValue>
        <ActionAttributeDesignatorAttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id" DataType="http://www.w3.org/2001/XMLSchema#string"/>
      </ActionMatch>
    </Actions>
  </Target>
</Rule>
Policy File for Location LNT:

<?xml version="1.0" encoding="UTF-8"?>

<!--Document: CityLNT.xmlCreated on: November 13, 2007, 9:30 AMAuthor: yxh068000Description:Purpose of the document follows.-->


<Description>This policy file specifies the rules to be evaluated for a user accessing the locationLNT based on the division the user belongs to and the severity of the emergency.</Description>

<Target>

<Subjects>

<AnySubject/>

</Subjects>

/Resources>

<AnyResource/>

</Resources>

<Actions>

<AnyAction/>

</Actions>

</Target>

</Policy>
<Rule RuleId="Emergency:Gov1" Effect="Permit">
  <Description>
  Government 1 agencies can access this location at severity level 3.
  </Description>
  <Target>
  <Subjects>
    <Subject>
      <SubjectMatchMatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal"><AttributeValue
          DataType="http://www.w3.org/2001/XMLSchema#anyURI">http://Route-Finder.com/emergency/Level-3/GOV1</AttributeValue>
      <SubjectAttributeDesignatorAttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id" DataType="http://www.w3.org/2001/XMLSchema#anyURI"/>
    </SubjectMatch>
  </Subjects>
  <Resources>
    <Resource>
      <ResourceMatchMatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal"><AttributeValue
          DataType="http://www.w3.org/2001/XMLSchema#anyURI">http://Route-Finder/CityLNT</AttributeValue>
      <ResourceAttributeDesignatorAttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id" DataType="http://www.w3.org/2001/XMLSchema#anyURI"/>
    </ResourceMatch>
  </Resources>
  <Actions>
    <Action>
      <ActionMatchMatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal"><AttributeValue
          DataType="http://www.w3.org/2001/XMLSchema#string">access-route</AttributeValue>
      <ActionAttributeDesignatorAttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id" DataType="http://www.w3.org/2001/XMLSchema#string"/>
    </ActionMatch>
  </Actions>
</Target>
</Rule>

<Rule RuleId="Emergency:Gov1" Effect="Permit">
  <Description>
  Government 1 agencies can access this location at severity level 2.
  </Description>
  <Target>
  <Subjects>
    <Subject>
      <SubjectMatchMatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal"><AttributeValue
          DataType="http://www.w3.org/2001/XMLSchema#anyURI">http://Route-Finder.com/emergency/Level-2/GOV1</AttributeValue>
      <SubjectAttributeDesignatorAttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id" DataType="http://www.w3.org/2001/XMLSchema#anyURI"/>
    </SubjectMatch>
  </Subjects>
  <Resources>
    <Resource>
      <ResourceMatchMatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal"><AttributeValue
          DataType="http://www.w3.org/2001/XMLSchema#anyURI">http://Route-Finder/CityLNT</AttributeValue>
      <ResourceAttributeDesignatorAttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id" DataType="http://www.w3.org/2001/XMLSchema#anyURI"/>
    </ResourceMatch>
  </Resources>
  <Actions>
    <Action>
      <ActionMatchMatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal"><AttributeValue
          DataType="http://www.w3.org/2001/XMLSchema#string">access-route</AttributeValue>
      <ActionAttributeDesignatorAttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id" DataType="http://www.w3.org/2001/XMLSchema#string"/>
    </ActionMatch>
  </Actions>
</Target>
</Rule>
Government 2 agencies can access this location at severity level 3.
<Rule RuleId="Emergency:Gov3" Effect="Permit">
  <Description>
    Government 3 agencies can access this location at severity level 3.
  </Description>
  <Target>
    <Subjects>
      <Subject>
        <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal">
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#anyURI">http://Route-Finder.com/emergency/Level-3/GOV3</AttributeValue>
        </SubjectMatch>
      </Subject>
    </Subjects>
    <Resources>
      <Resource>
        <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal">
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#anyURI">http://Route-Finder/CityLNT</AttributeValue>
        </ResourceMatch>
      </Resource>
    </Resources>
    <Actions>
      <Action>
        <ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">access-route</AttributeValue>
        </ActionMatch>
      </Action>
    </Actions>
  </Target>
</Rule>
<Rule RuleId="Emergency:Lnt" Effect="Permit">
<Description>
Users belonging to the LNT division can access this location at Severity level 3.</Description>
</Rule>

<Rule RuleId="Emergency:Lnt" Effect="Permit">
<Description>
Users belonging to the LNT division can access this location at Severity level 2.</Description>
</Rule>
<Subjects>
  <Subject>
    <SubjectMatchMatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal"><AttributeValue
      DataType="http://www.w3.org/2001/XMLSchema#anyURI">http://Route-Finder.com/emergency/Level-2/LNT</AttributeValue>
    <SubjectAttributeDesignatorAttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"DataType="http://www.w3.org/2001/XMLSchema#anyURI"/>
  </SubjectMatch>
  </Subject>
</Subjects>

<Resources>
  <Resource>
    <ResourceMatch
      MatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal"><AttributeValue
      DataType="http://www.w3.org/2001/XMLSchema#anyURI">http://Route-Finder/City-LNT</AttributeValue>
    <ResourceAttributeDesignatorAttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"DataType="http://www.w3.org/2001/XMLSchema#anyURI"/>
  </ResourceMatch>
  </Resource>
</Resources>

<Actions>
  <Action>
    <ActionMatch
      MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal"><AttributeValue
      DataType="http://www.w3.org/2001/XMLSchema#string">access-route</AttributeValue>
    <ActionAttributeDesignatorAttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"DataType="http://www.w3.org/2001/XMLSchema#string"/>
  </ActionMatch>
  </Action>
</Actions>

<Rule
  RuleId="Emergency:Lnt"
  Effect="Permit">
  <Description>
    Users belonging to the LNT division can access this location at Severity level 1. </Description>
  <Target>
    <Subjects>
      <Subject>
        <SubjectMatchMatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal"><AttributeValue
          DataType="http://www.w3.org/2001/XMLSchema#anyURI">http://Route-Finder.com/emergency/Level-1/LNT</AttributeValue>
        <SubjectAttributeDesignatorAttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"DataType="http://www.w3.org/2001/XMLSchema#anyURI"/>
      </SubjectMatch>
      </Subject>
    </Subjects>
  </Target>
</Rule>
<Resources>
  <Resource>
    <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal"><AttributeValue
      DataType="http://www.w3.org/2001/XMLSchema#anyURI">http://Route-Finder/CityLNT</AttributeValue>
    </ResourceMatch>
  </Resource>
  <Resource>
    <ResourceAttributeDesignatorAttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id" DataType="http://www.w3.org/2001/XMLSchema#anyURI"/>
  </Resource>
</Resources>

<Actions>
  <Action>
    <ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal"><AttributeValue
      DataType="http://www.w3.org/2001/XMLSchema#string">access-route</AttributeValue>
    </ActionMatch>
  </Action>
</Actions>
</Target></Rule></Policy>