Axiomatics

Axiomatics, located in Stockholm, Sweden and Salt Lake City, USA, provides fine-grained and attribute-based authorization (ABAC) solutions based on the XACML standard. The company has a global customer base within healthcare, finance, manufacturing and the public sector, among others. The company’s solutions help protect systems against unauthorized use while enabling secure sharing of information within and across enterprise borders through the use of extensible and externalized authorization. Axiomatics actively contributes to the development of the XACML standard and has editorial responsibilities within the OASIS Technical Committee.

The Axiomatics Extension for CA SiteMinder® utilizes the existing CA SiteMinder Authorization API for its integration. The integration enables CA SiteMinder users to include XACML 3.0 conformant policy evaluation on all incoming access requests. Since version 3.0 of the OASIS XACML standard just recently has been approved by the XACML Technical Committee and the standard itself gets considerable attention on the market, this extended functionality may be of interest for existing CA customers. Furthermore, it may strengthen CA’s offering when XACML capabilities are explicitly being asked for in a new business case and XACML 3.0 conformance is a differentiator.

Organizations with complex data sharing requirements such as health care, financial services, insurance, highly regulated industries and government agencies will benefit from the policy driven approach to data access. Other applications such HR, Payroll, Expense Management, and a broad variety of corporate portals, will enjoy the flexibility of attribute based authorization.

Integration Summary

The CA SiteMinder Authorization API can be used to extend authorization capabilities to include factors that are external to the request context itself using dynamic active policies. Users can write Java code to interact with other information systems to retrieve data needed to help the SiteMinder Policy Server to reach a decision on whether access should be granted or denied. The Java class of the extension is registered to be invoked by an active policy.

The Axiomatics extension provides a ready integration component which utilizes this Authorization API. It retrieves the request context from CA SiteMinder and transforms it into an XACML access request. The XACML requests is sent to the XACML-based Axiomatics Policy Decision Point (PDP) which responds with a PERMIT or DENY depending on the evaluation of the XACML policies it is configured with. This response is returned to the CA SiteMinder Policy Server the same way any custom-built active policy conformant with the Authorization API returns a response.

To implement new dynamic authorization capabilities into CA SiteMinder, users simply include the Axiomatics Extension for CA SiteMinder in their active policy definitions and then load appropriate XACML policies into the Axiomatics PDP.

In comparison with writing custom Java extensions, the Axiomatics approach brings a number of obvious advantages:

- **Speed of deployment:** Adding a new dynamic policy only requires the XACML policy to be modeled based on the corresponding business rule. No code needs to be written.
- **Maintenance:** a change in regulatory requirements or corporate directives can be implemented via new or altered XACML policies without any change whatsoever to deployed applications or any Java custom code.
Auditing and governance: XACML is standard-based and auditable. Axiomatics also offers the Axiomatics Policy Auditor, which can be used to verify deployed policies. For Java code embedded in custom extensions any auditing is comparatively much more difficult to achieve.

Externalization: The Axiomatics Policy Server comes out of the box with GUI support for integration with external sources via LDAP or SQL queries. Other types of interactions with the surrounding infrastructure can easily be added as well. Naturally, custom Java code can access other data sources as well, but the standards-based way makes it faster, easier and more transparent.

Architecture

The end-user request is captured by a CA SiteMinder agent which forwards the request to the CA SiteMinder Policy Server. If the request realm or component in CA SiteMinder Policy Server is configured to use an Active Policy that calls the Axiomatics Extension, the request is automatically forwarded to the Axiomatics Policy Server PDP where the final evaluation is made against deployed XACML policies.

System Requirements

The Axiomatics Extension for CA SiteMinder is deployed on any CA SiteMinder server and runs in the environment of CA SiteMinder. Its system requirements are thus the same as for CA SiteMinder. The extension (PEP) adds very little additional overhead with regard to memory or CPU load but may of course in some instances motivate that resources are added to the hardware it runs on.

The Axiomatics Policy Server runs on JEE application servers such as Tomcat or WebSphere. It supports a broad range of deployment scenarios for high-availability. For details, please refer to the Axiomatics Policy Server data sheet which can be downloaded from here:

The Axiomatics Policy Server product and its various additional components is described in detail on the product pages of the Axiomatics web site:

http://axiomatics.com/axiomatics-products-overview.html

Axiomatics products in general are Java based and run on Tomcat or WebSphere, and on Windows or Linux systems. For .NET environments, PEP components are available.

PDPs are typically deployed as authorization services on a container. However, they can also be embedded with their PEPs. Such scenarios have not been considered in the initial release of the CA SiteMinder integration. If such demands exist, please contact Axiomatics Professional Services.

The integration supports CA SiteMinder 12.5 and later with Axiomatics Policy Server 5.0 or later.

### Integration Details

The Axiomatics Policy Decision Point (PDP) has configurable Policy Information Points (PIPs) which retrieve data from external sources. The product comes with an interface for LDAP and SQL sources built-in. Administrators define LDAP or SQL queries in a graphical user interface for attribute sources. They thereby automate the retrieval of attributes needed for the Axiomatics PDP’s policy evaluation.

XACML policies are written in either of the two Policy Administration Points delivered with the product: the PAP GUI which is an advanced IDE for XACML policy authoring with testing and debugging features or the ALFA plugin for Eclipse which uses the Axiomatics Language for Authorization (ALFA), a human-readable and user friendly way to produce XACML policies.

To enable XACML-based authorization of an application that is protected by CA SiteMinder, the following steps would be needed:

- Install the Axiomatics Extension. The installation very simple – you copy a set of .jar files into the file structure of a CA SiteMinder Policy Server instance and update corresponding configuration files. Files to add:
  
  ```
  ../../../siteminder/bin/thirdparty/axiomatics
  axiomatics-pep-sdk-for-java.jar
  axio-xacml.jar
  axio-xacml-request-api.jar
  commons-io.jar
  commons-logging.jar
  common-pool.jar
  geronimo-javamail_1.4_spec.jar
  icu4j.jar
  siteminder-pep.jar
  xmlsec.jar
  config/
    pdp.properties
    log4j.properties
  ```

  In addition to the above two configuration files you need to update:

  ```
  /siteminder/config/JVMOptions.txt
  ```
• Import CA SiteMinder attributes into the Axiomatics Policy editor you want to use – these attributes are included in the extension package.

• Write your XACML policy using SiteMinder attributes and whatever external attributes you need.
Optionally: define PIP connectors to retrieve attribute values from external LDAP or SQL sources if such attributes are used in your policy – for details see the Sample Use Case Scenario below.

Define an active policy in CA SiteMinder that uses the Axiomatics Extension

**Sample Use Case Scenario**

A sample use case scenario can be borrowed from the CA Technology Brief from April 2011, "CA SiteMinder® prepares you for what’s ahead", page 12:

"Custom conditions can be evaluated using active policies to achieve even more fine-grained control over authorization. For example, a policy could deny access to an order entry page for customers with an overdue balance in an accounting database."

(Source: http://www.ca.com/~media/Files/TechnologyBriefs/casiteminder-tb-final-4-11.pdf)

In this use case we have the following external factors that must be considered in order to make a policy decision:

- The current user’s (SiteMinder %SM_USER) affiliation with a customer ID may need to be established through a query to an external database or directory.
- The company’s balance in the accounting database must be checked.

An XACML policy to enforce this rule would express:

```
DENY user to POST (%SM_http-action=POST) order entry page (%SM_http-request-uri=[order entry form action URL]) if user(%SM_USER)->customer’s account balance is overdue (%PIP_balance<0)
```

The action, HTTP POST, the resource URL (the form action) and the user ID are all contained in the request context to which CA SiteMinder has access. These attributes are all retrieved by the Axiomatics extension from CA SiteMinder, denoted with names starting with %SM_ above.

The reason an active policy would need to use custom authorization is that the balance of the user (or rather the company to which the user belongs) must be retrieved from an external source. In the above notation we’ve called this attribute the %PIP_balance, indicating that an Axiomatics Policy Server PIP is configured to lookup the balance.

A PIP like this is easily configured in the Axiomatics Services Manager GUI:

1. Create the PIP connector in the Axiomatics Services Manager:
2. Configure it in the Axiomatics Services Manager:

3. The company ID of the customer which owns the account also needs to be resolved. This could come from either of these two sources:
   a. CA SiteMinder has access to the customer ID via the identity store which is used for user authentication. This could for instance be a corporate LDAP. If so, CA SiteMinder passes the Company ID along with the identity of the user in the request.
   b. The company ID is retrieved via yet another PIP which for instance passes the %SM_USER in the SQL statement or LDAP query that retrieves the user’s company ID from a database or directory.

The Axiomatics Extension for CA SiteMinder automates the retrieval of whatever attributes the SiteMinder request context contains and sends them in a request to the Axiomatics PDP. The Axiomatics PDP evaluates its policies and returns a PERMIT or DENY. During the evaluation process, the Axiomatics PDP automatically will retrieve whatever external attributes it needs as well via its configured PIPs – in the example above the balance and possibly the company ID.
Contact Information

Axiomatics, Inc.
1338 S Foothill Drive #237
Salt Lake City, UT 84108
Phone: +1 801 55 69 994

Email: support@axiomatics.com
Website: www.axiomatics.com

CA Technologies
One CA Plaza
Islandia, NY 11749
Phone: 800-225-5224
Fax: 631 342-6800

Email: TechnologyPartnerProgram@ca.com
Website: support.ca.com

Support

Axiomatics Customer Support is available at:

https://support.axiomatics.com

Appendices

For additional information, please refer to the Third Party Extensions section and the CA SiteMinder page on the Axiomatics corporate web site at www.axtiomatics.com.