White Paper

Cybercom & Axiomatics Joint Identity & Access Management (R)evolution

Federation and Attribute Based Access Control

AXIOMATICS

Realization of the IAM (R)evolution

Executive Summary

Many organizations are currently striving to develop new strategies for their Identity & Access Management (IAM) implementations. While investments made need to be leveraged, they look for IAM capabilities that will make them more agile and responsive to rapidly changing requirements.

Where existing IAM technologies and procedures focus on abilities to **restrict** access, organizations are more challenged with the need to **share** information and to **collaborate** across organizational borders in a secure manner. Where existing IAM infrastructures offer a **static** and **coarse-grained** set of access configurations, business processes demand a more **dynamic** and **fine-grained** approach. Capabilities to speed-up deployment of new services are also needed.

The reasons for this and a high-level discussion regarding available technical options have been presented in a separate white paper – The IAM (R)evolution – which identifies two important technical trends to consider:

- **Federated identity management**
- **Attribute Based Access Control (ABAC)**

Combined, these technologies allow an organization to achieve the above outlined goals while protecting the value of investments already made.

The new concept is **revolutionary** in the sense that it provides a new level of abstraction and logic in access management. Rather than having to manage access for individual know users or groups/roles of known users, corporate policies can be translated into XACML policies and enforced within IT systems based on descriptive attributes that are generally applicable to currently known as well as future unknown users and information assets.

However, the change represents an **evolution** in the sense that investments made in centralized identity management, role engineering and information classification will be fully leveraged.

This document describes a technical platform provided jointly by Cybercom and Axiomatics with which the outlined IAM (r)evolution can be realized. It uses the Cybercom Enhanced Security Platform (CESP) for federation and attribute management and integrates with Axiomatics Policy Server (APS) for attribute-based access control and XACML.

Federated Identity Management

Federated Identity Management is a term used to describe a service oriented approach to identity management whereby functional services and identity services are separated:

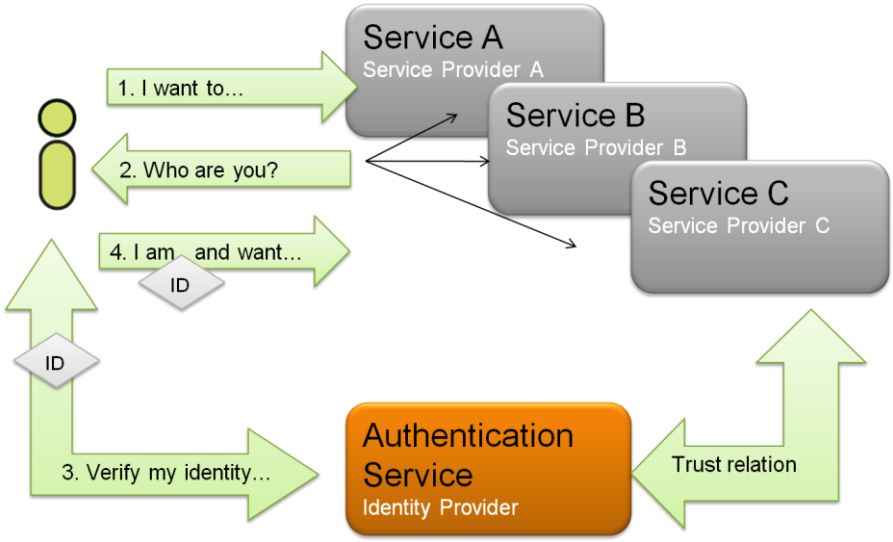

Figure 1: Federation

© Axiomatics AB, 2010

Cybercom Enhanced Security Platform (CESP)

The Cybercom solution includes a full-blown engine for federation of identities combined with a set of tools and components to connect this federated environment to other related attribute sources and directories.

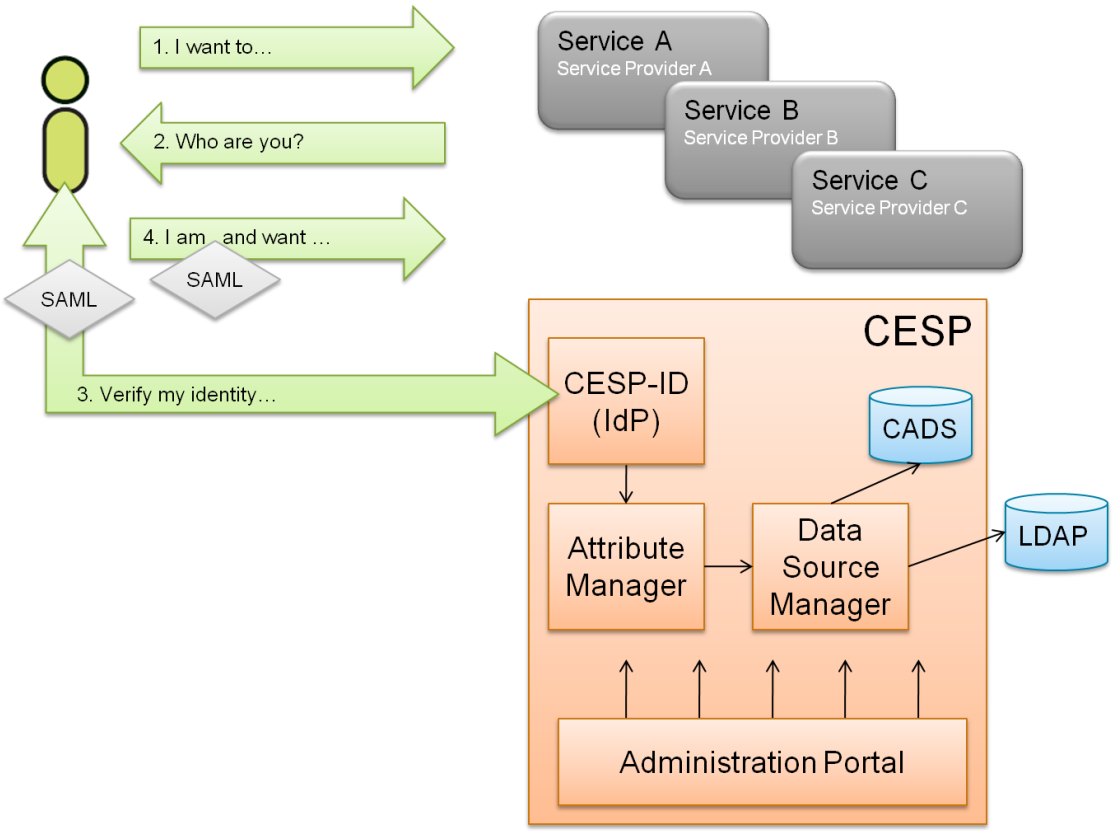

Figure 2: Cybercom Enhanced Security Platform

The CESP-ID component is a SAML 2.0 compliant Identity Provider which authenticates principals such as end-users, services or applications which prove their identities to CESP-ID by presenting the necessary credentials. CESP-ID can be configured to accept a variety of credentials ranging from user name / password to various schemes of strong authentication using X.509 certificates or various types of tokens or one-time passwords.

On successful authentication, CESP-ID issues a SAML token to the authenticated principal. Service providers with a trust relation to the CESP-ID can redirect users to the CESP portal for authentication and then accept the SAML token on login.

The CESP-ID component in turn is connected to the existing infrastructure and utilizes information already maintained in corporate LDAP directories or databases. In this sense, the CESP platform can be seen as a virtual directory which filters out identities and related attribute data that can be relevant when SAML tokens are being issued.

CESP provides the administrative interface for the solution to enable administrators to

- Select and connect to authoritative data sources in the existing infrastructure via the Data Source Manager
- Select the attributes sources that need to be tied to user identities at logon when SAML tokens are issued via the Attribute Manager.

Important capabilities and functions from a federation perspective provided by CESP include

- An administrative interface for federated identity management
- Centralized authentication services and thus single sign-on for users

© Axiomatics AB, 2010

- Centralized logging of user authentications
- Control and audit capabilities

In addition, CESP comes with essential supporting functions such as means to establish secure communication across network boundaries, server management and notification services to support business continuity related processes and secure infrastructure maintenance.

For a more detailed description of CESP capabilities, please refer to the Cybercom White Paper Cybercom Enhanced Security Platform.

Attribute Based Access Control (ABAC)

ABAC introduces authorization as an application-external and standardized service in much the same way as federation offers authentication as a service externalized from applications.

ABAC makes use of the XACML standard which provides

- **A general request/response language** for authorization questions.
- **A general policy language** which allows administrators to author corporate policies in an exact language that enables secure evaluation of XACML access requests.
- **A reference architecture** as outlined below**:**

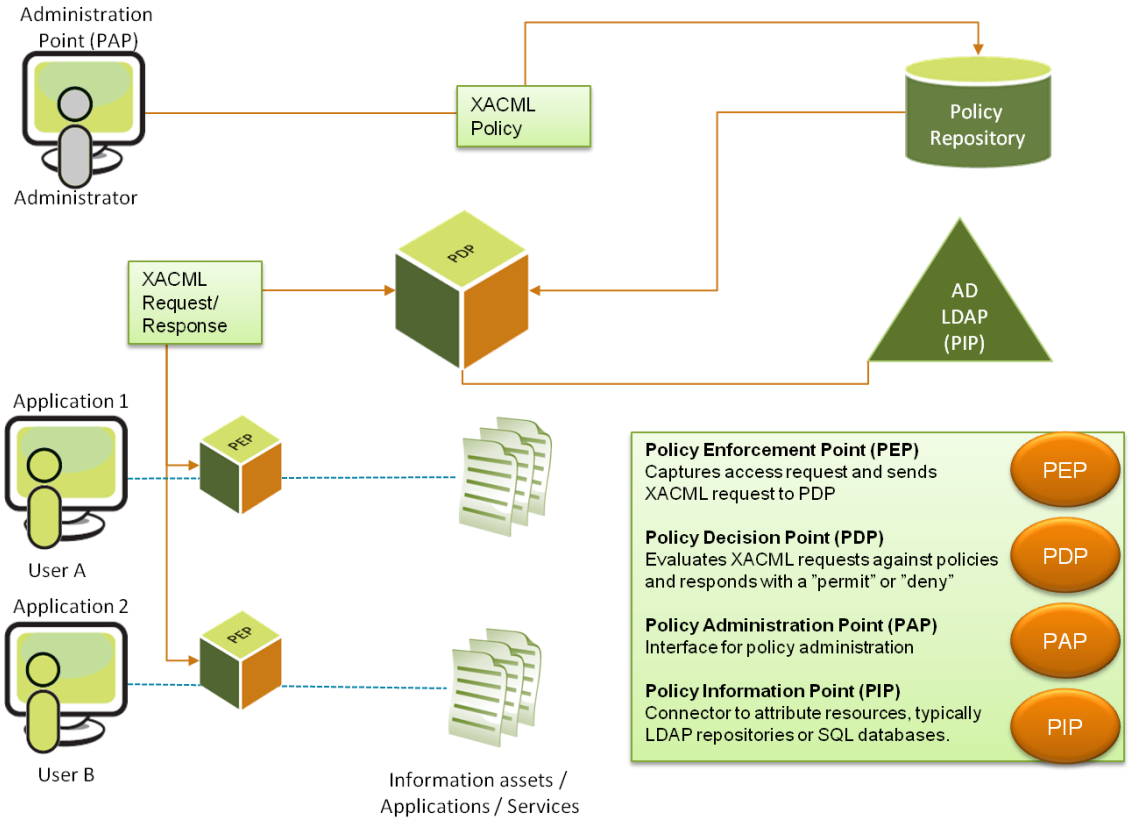

Figure 3: Attribute Based Access Control / XACML reference architecture

Axiomatics Policy Server (APS)

Axiomatics Policy Server (APS) implements XACML compliant software modules that reflect the above reference architecture. APS is completely consistent in standard compliance. This means it stores policies in XACML and only uses XACML compliant methods for policy evaluations. The APS product includes the following components:

- **PAP:** An administrative graphical user interface for policy authoring with advanced features to support simulation of access requests and debugging of XACML policies. The Axiomatics PAP

© Axiomatics AB, 2010

can be thought of as an IDE for XACML policy developers. It also includes a rich set of functions to support governance in policy maintenance. Policy life-cycles are maintained with a complete history of events. Once a policy is put in production it cannot be altered – if changes are necessary updated versions will replace the securely archived original.

- **PDP:** A policy engine that accepts XACML requests and evaluates them against the XACML policies in its policy repository. The PDP normally runs on an application server but other options such as closely coupled PEP/PDP deployments whereby the PDP runs in-process with its PEP are also supported. The Axiomatics PDP is available both for Java and .NET environments. It uses advanced optimization techniques to boost performance.
- **PIP:** An attribute finder interface through which the Axiomatics PDP can be configured to access external attribute sources during policy evaluation.
- **PEP:** A set of basic enforcement components for different environments and integration scenarios.

CESP and APS combined

Axiomatics Policy Server (APS) can be deployed as a component fully integrated within the Cybercom Enhanced Security Platform (CESP), as illustrated below.

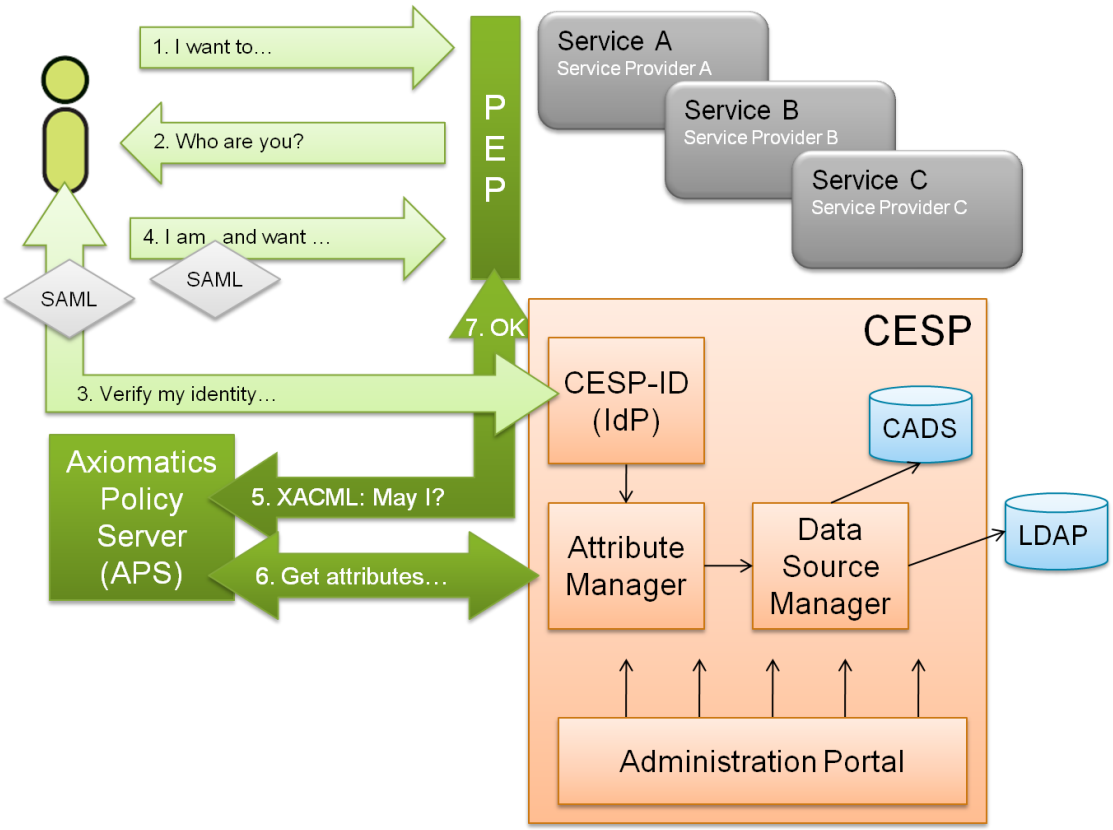

Figure 4: APS running within the Cybercom Enhanced Security Platform CESP

Running in this environment, APS benefits from the rich management features provided by the platform. The CESP already delivers essential management functions for the administration of privilege-giving attributes to be included in SAML tokens. With the two environments integrated, attribute management features offered by the CESP such as the Attribute Manager, the Data Source Manager and the Attribute Data Store (CADS), add vital administrative support functions to the APS environment as well.

Via the Data Source Manager, privilege-giving attributes needed for XACML policy evaluation can be added to the CESP domain.

The Axiomatics PIP interface can utilize the CESP as the single trusted authority for its attribute retrieval. The Attribute Manager within the CESP platform thus serves as a virtual directory feeding the Axiomatics PDP.

© Axiomatics AB, 2010

The following chain of events illustrates how the CESP/APS combination delivers externalized authentication and authorization services for an application or service:

1. User connects to the desired service (through a client application or browser interface).
2. Service redirects the user to CESP-ID for authentication.
3. User presents credentials to CESP-ID, becomes authenticated and receives a SAML token.
4. User is referred back to the service.
5. The service provider accepts the user's SAML token and grants access to the service.
6. The user request is now intercepted by the XACML PEP which translates the request to an XACML authorization request which is sent to the Axiomatics PDP. The XACML request includes the attributes of the SAML token provided by CESP-ID.
7. The Axiomatics PDP evaluates the user request against XACML policies. If additional attributes are needed for policy evaluation, the Axiomatics PIP interface queries the CESP attribute manger. Once all attributes for policy evaluation have been gathered, the PDP responds with a "permit" or "deny" and the PEP grants or refuses access accordingly.

Conclusions

Axiomatics Policy Server (APS) and the Cybercom Enhanced Security Platform (CESP) combined deliver authentication and authorization as a service.

Connectors provided by CESP enable efficient integration with existing identity management systems, directories and other attribute sources. CESP and APS combined can therefore be used to consolidate existing identity and access management infrastructures and to leverage investments made.

The service oriented approach to authentication and authorization help organizations overcome problems with **static** and **coarse-grained** access configurations and to respond to business demands for a more **dynamic** and **fine-grained** approach.

Furthermore, the CESP / APS solution provides capabilities to speed-up and simplify deployment of new services in a cost-efficient manner.

In SOA environments, developers can focus on functional requirements rather than having to hard-code authentication and authorization schemes into their applications which reduces time and costs in new service deployments.

With a policy-based approach to authorization, regulatory compliance can be achieved, enforced and verified for multiple information systems from a central point.

© Axiomatics AB, 2010