June 2008
Volume 1, Issue 2

DoD COI Newsletter

DoD CIO Information Policy & Integration Directorate

Turbo-Charging Information Access through ABAC

Getting access to information is too hard. Today, users typically must register with each data system before they can access the mission critical information they need. This process frequently takes days. And since each system maintains a separate copy of the user's information, it's a process rife with potential security issues. Equally problematic – information owners find it difficult to quickly make their data accessible to new users. They have to wait for each user to submit required information and paperwork. Luckily, there's a better way on the horizon; it's called Attribute-Based Access Control or ABAC.

ABAC expedites access to information and services by leveraging information or attributes about users from authoritative sources. Figure 1 (page 2) illustrates this process. When a user requests access to a resource's information or services, a wrapper associated with the resource called a Policy Enforcement Point (PEP) invokes the resource's Policy Decision Point (PDP) to determine if the user can access the resource. The PDP retrieves the user's attributes from authoritative, trusted sources and then enforces resource-specific policies that consider user and resource attributes to determine if a user may access the resource at this time. In this way, users who have not previously registered with the resource, commonly referred to as unanticipated users,

Continued on page 2

COI Spotlight: Acquisition Visibility

February 29, 2008 marked the start of change in the way DoD manages its Defense acquisition data. On that day, three acquisition oversight tools were able to display authoritative major weapons systems (MWS) data from 12 Major Defense Acquisition Programs (MDAPs), on demand, providing information to support acquisition oversight for $103B in total program value.

Earned Value Management (EVM) and unit cost data for 12 MDAPs, four from each Service[1], were obtained from the authoritative source for each data element, in real time. Community Of Interest (COI) activities were foundational to this accomplishment. As part of an MWS COI, representatives from each of the Services participated in determining the definitions of the data elements to be obtained for each program, designated authoritative sources for each data element, and assigned responsibility for maintaining the authoritative copy of each data element in its source system.

USD(AT&L) officially initiated this effort by memorandum, dated October 5, 2007, mandating a Service-Oriented Architecture (SOA) Demonstration Project, to be led by Mr. Gary R. Bliss, AT&L, ARA, with Service participation. Providing strategic functional vision and leadership, Mr. Bliss established the foundational data governance and management concepts and methodologies to be employed. Mr. Mark Krzysko, AT&L, BT, co-led with a focus on data management and organizational implementation. He also provided technical vision and leadership, establishing the SOA middleware framework and SOA infrastructure required for the Demo. AT&L, BT formalized the ATL AV (Acquisition Visibility) COI in February 2008 to continue supporting Defense acquisition data governance during the ongoing AT&L SOA pilot activities and into implementation of a Defense acquisition data management capability.

The successful demonstration of data governance and technical capability offers the Department the opportunity to fundamentally change for the better the Department's ability to make informed Acquisition decisions based on timely and authoritative data.

Mark Krzysko
Mark.Krzysko@osd.mil

Announcements

Next COI Forum
- 9 July 2008

COI/Data Sharing/ Training
- 15 – 16 July 2008
- For registration e-mail :COI_HelpDesk@osd.mil

DoD CIO IP&I

1851 S. Bell Street
Suite 600
Arlington, VA 78269

E-MAIL:
COI_HelpDesk@osd.mil

COI Resources on the Web!

See us at:

http://www.dod.mil/cio/coi/

Information Access through ABAC *continued from page 1*

can access resources on-the-fly. Equally important, resources can ensure that users who do not currently have the appropriate attributes cannot gain access, even though they may have been granted access in the past, and that all users who do have the appropriate attributes, even if they are unknown to the resource, will be granted immediate access.

ABAC builds on other enterprise capabilities, such as public key infrastructures and service-oriented architecture frameworks, but its success primarily depends on the availability of trustworthy and accurate attribute repositories. Both the Department of Defense (DoD) and Intelligence Community (IC) are developing enterprise-wide, authoritative repositories known as the Joint Enterprise Directory Service (JEDS) and the Full Service Directory (FDS), respectively. The list of attributes to be included in these directories is being guided by the joint Authorization and Attribute Service Tiger Team (AATT).

ABAC is rapidly becoming a reality. The AATT expects to finalize a joint set of ABAC attributes and service interfaces in FY08. Initial versions of these capabilities have already been demonstrated in the 2008 Joint Expeditionary Force Experiment (JEFX) and will be further demonstrated in Empire Challenge 2008 - both sponsored collaboratively by the USD(I), DoD CIO, the Distributed Common Ground System (DCGS) Family of System teams, and the Net-Centric Enterprise Services (NCES) team in response to Program Decision Memorandum (PDM) II & III direction. The capabilities will become operational with the deployment of NCES Increment 1 services and with the release of DCGS Infrastructure Backbone (DIB) Version 1.3, which are planned for early to mid-2009.

To learn more about how the DoD is using ABAC to turbo-charge information access, please contact Mike Moore (john.moore@osd.mil) or Myra Powell (myra.powell@osd.mil) from the DoD-CIO team.

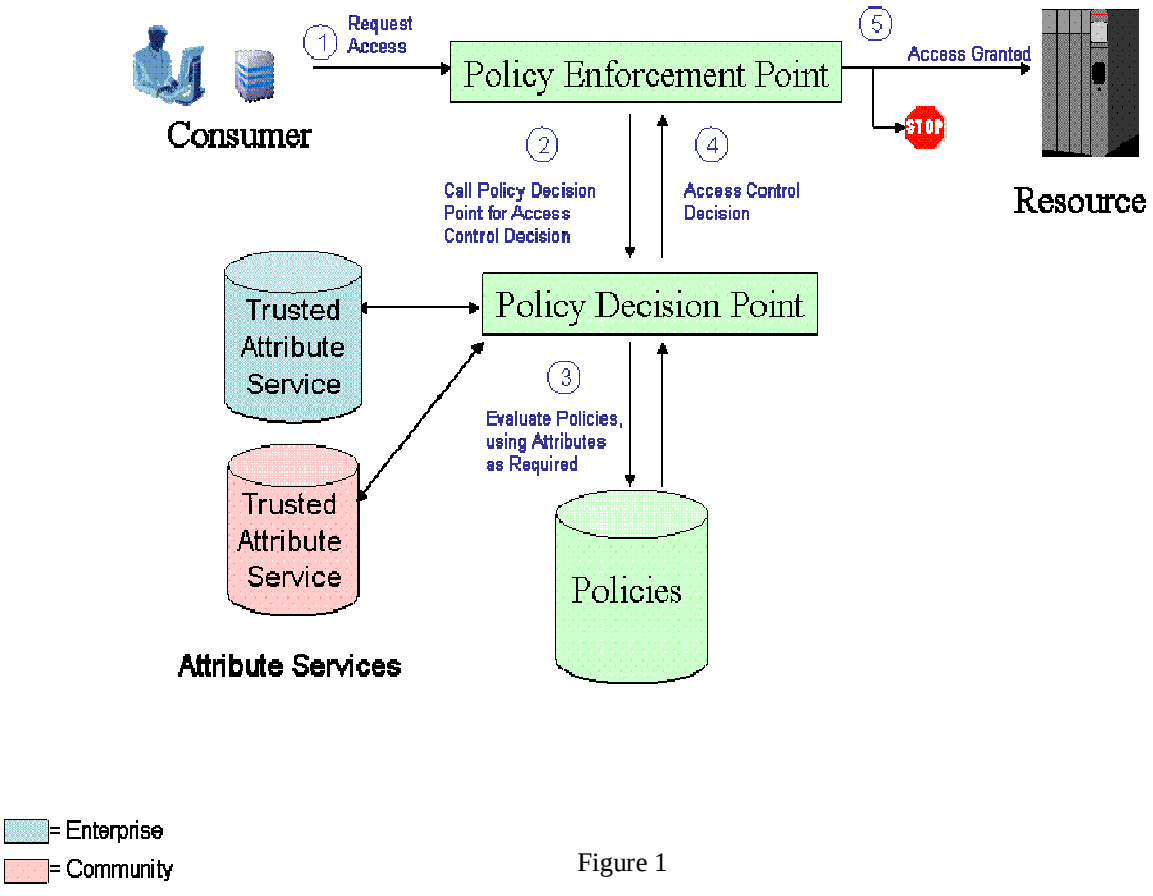

Figure 1