AXIOMATICS FEDERAL

Use Case

Federal mission: Dissemination and Information Sharing using Attribute Based Access Control (ABAC)

Mission

The U.S. federal intelligence community (IC) functioned for many years in a "need-to-know" culture, where intelligence information was closely guarded within each agency. These information silos were necessary for the Cold War when information protection was paramount, but became a hindrance in post 9/11 America where the aggregation of disparate intelligence data and the cross-agency collaboration of data was often needed to identity threats and complete mission objectives.

To address this new challenge, IC leadership mandated that intelligence information be more readily shared across the community, while still protecting this shared data from unauthorized access.

Dr. Dale Meyerrose, former Associate Director of National Intelligence/Intelligence Community Chief Information Officer (CIO) and Information Sharing Executive for the DNI, said "This new information sharing model will rely on attribute-based access and tagged data with security built-in to create a trusted environment for collaboration among intelligence professionals to share their expertise and knowledge."[1]

A new access control model was needed to provide Attribute Based Access Control and facilitate the dissemination and sharing of intelligence data.

About Axiomatics Federal, Inc.

Axiomatics works with U.S. federal agencies to help them meet their access control needs. Through a policy-based approach to dynamic authorization that implements the Attribute Based Access Control (ABAC) model, Axiomatics helps government agencies in Defense, Intelligence, and Civil sectors meet the need to lock down sensitive data while securely sharing with authorized users.

The Specifics

What: U.S. federal agencies can address dissemination and information sharing across other agencies by managing access to sensitive data with dynamic, attribute-based authorization.

Why: Axiomatics is the leader in fine-grained, externalized authorization management (EAM): the most adaptable and scalable way to solve data security concerns. Today, leading automotive, pharmaceutical, banking, and defense manufacturers use our solutions to safeguard and share sensitive data. Our products are used in several U.S. federal agencies to leverage the advantages offered by fine-grained access control.

Who: Axiomatics is the leader in fine-grained, externalized authorization management (EAM): the most adaptable and scalable way to solve data security concerns. Today, leading automotive, pharmaceutical, banking, and defense manufacturers use our solutions to safeguard and share sensitive data. Our products are used in several U.S. federal agencies to leverage the advantages offered by fine-grained access control.

How: Axiomatics provides a suite of solutions that enforce dynamic authorization—at the application, API, and data layers—from one centrally managed point. We consider the full context under which a user wishes to access data, and permit or deny access accordingly.

With a centralized authorization service, advanced auditing and reporting tools also ensure compliance is met on an ongoing basis, while real-time controls allow policy changes to be instantly enforced to meet rapidly changing regulatory environments.

[1]ODNI Information Sharing Strategy, February 22, 2008 (https://fas.org/irp/dni/iss.pdf)

A Dissemination Use Case in Action

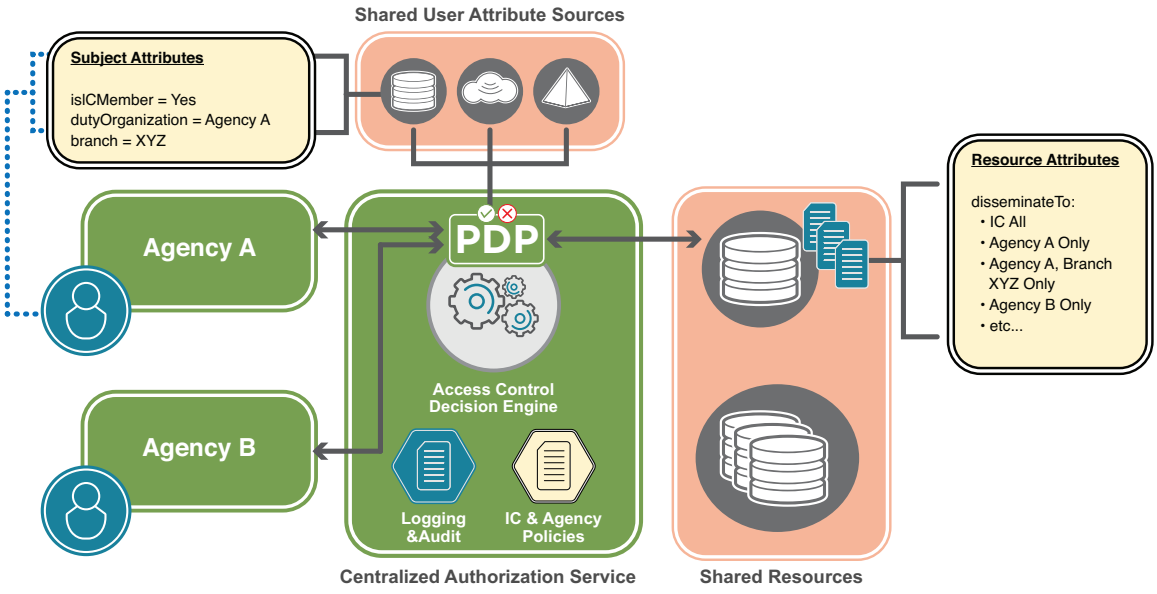
A federal agency can take advantage of the strengths of Attribute Based Access Control (ABAC) to help with the dissemination and sharing of intelligence data.

Agencies curate large volumes of data. Per the direction given by the ODNI, best efforts must be made to share this data throughout the IC, with exceptions needing to be justified and approved. To process these exceptions, there must be metadata that describes aspects of the data to differentiate it from shareable data. Furthermore, policies must exist that can evaluate the characteristics (attributes) of the requestor of the data, the data being requested, and what the requestor wants to do with the data (e.g. discover, read, delete).

ABAC achieves this by considering the context of the access control request. Context is defined as using subject, resource, and environmental attributes to process digital policies to obtain an access control decision dynamically and at run-time. This allows for complex policy algorithms that can consider the *who, what, when, where, why,* and *how* of an access request, instead of just focusing on the *who* and the *what*. ABAC policies can be expressed in Boolean rules that allow for complex analysis of attributes and in determining how the rules are combined to accurately reflect agency policies.

With an ABAC approach, there is virtually no limit to the granularity of the protected data. To make an access control decision, a policy simply needs some information about that data. Therefore, access control decisions can be made at the row, column, document, paragraph, and even cell level of your stored data. By labeling as sensitive the data at a paragraph level, for example, the remainder of a document can be shared with the Community using ABAC policies to enforce that the sensitive paragraph is not shared outside of your agency. Prior to ABAC, entire databases were locked down due to potentially only a small portion of the data being sensitive.

For example, consider the notional diagram below. By using shared user attribute sources and shared data resources, an externalized authorization service can render access control decisions based on IC and agency policies. Here we are using the fictional *disseminateTo* attribute as metadata attached to documents. Attribute values for *disseminateTo* could include IC ALL, Agency A Only, Agency B Only, etc., for use in broadening the dissemination of a piece of data, or restricting access to a narrower range. In this model, it is the data owner or steward who controls the access control for the data that he or she owns. In this example, if a document's *disseminateTo* attribute is set to a value of "Agency A, Branch XYZ Only," then only individuals with subject (user) attributes that identify them as IC members, within Agency A, Branch XYZ may access that document.



In summary, attributes and policies can be created and tailored to meet the specific access control requirements of your government agency. By using an ABAC approach in conjunction with a dynamic, externalized authorization service, agencies can progress towards a "responsibility to provide" mindset to better disseminate and share actionable intelligence to the Community.

11921 Freedom Drive
Reston, VA 20190
Tel: +1 (312) 374-3443

webinfo@axiomatics.com www.axiomatics.com twitter.com/axiomatics