AXIOMATICS FEDERAL

Use Case

Federal mission: Security Compliance using Externalized Authorization Management (EAM)

Mission

United States federal agencies are beholden to myriad regulations and standards, some of the most notable of which are the FIPS Publication 200 and the NIST Special Publication 800-53. Both documents, in combination, “ensure that appropriate security requirements and security controls are applied to all federal information and information systems.” These documents offer guidance on conducting an organizational IT risk assessment, and provide a template for determining what type of security controls are recommended to protect organizational operations and resources.

Federal IT systems are required to get Certification and Accreditation (C&A) to operate on federal agency networks. This process usually involves validating that the IT system meets the criteria established by a given agency’s IT security plan, tailored and derived from the NIST SP-800-53 initiative mentioned above. The entire process can be onerous, time-consuming, and expensive.

By using a centralized and externalized authorization management (EAM) service, the security accreditation process and the subsequent operations and maintenance can be shortened, saving time and money and allowing application developers to focus on the agency’s mission.

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 accelerate their Accreditation and Authorization (A&A) process by using 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: There are many internal stakeholders that benefit from a dynamic approach. ABAC helps assure CISOs and ISSOs that Access Control (AC) security controls are completed within the Security Requirements Traceability Matrix (SRTM) in accordance with the agency’s IT security plan. Compliance officers and auditors also take an active interest in how ABAC helps the agency meet and prove compliance.

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.

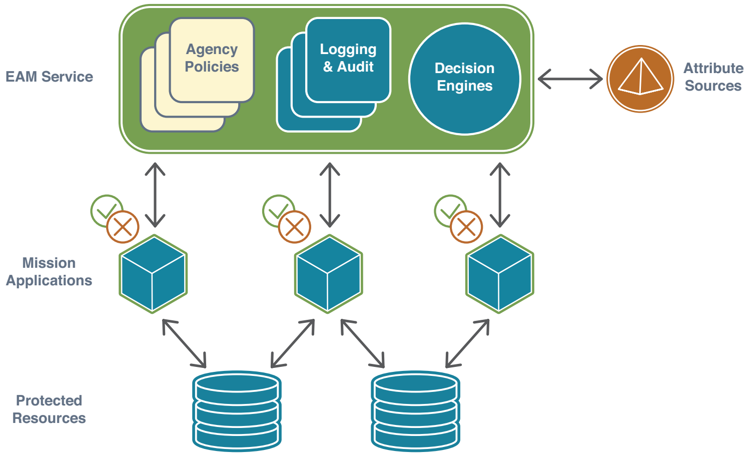
A Security Compliance Use Case in Action

Federal agencies that implement an enterprise, externalized authorization management (EAM) service realize a wide range of benefits, from fine-grained access control to centralized digital policy management. Improved security compliance, auditing, and monitoring are other compelling reasons to consider an EAM service.

Traditionally, federal enterprises comprise of mix of COTS (commercial) and GOTS (custom-built) applications to support their various missions. These applications are gateways to protected resources, such as sensitive health records, academic research, classified documents, and so forth. Each application must determine which users are permitted to access which resources. Over time, discrepancies invariably occur as to how accesses are handled across the enterprise. One application may allow access to one resource that is denied by another. Being able to answer the questions, “Who has access to what?” or “Who has accessed what?” becomes a near-impossible task. This leads to the even more challenging task of auditing and monitoring for security compliance.

By outsourcing the applications’ access control to a centralized service, a consistent means of authorization can be applied uniformly to all of the applications on an enterprise. This is achieved by transforming an agency’s natural language policies into digital policies, and the enforcing those policies through an EAM service, which contains a centralized digital policy management (DPM) store.

As shown in Figure 1, all the mission applications are shown subscribed to a centralized EAM service. Each application, which had to go through its own Accreditation and Authorization (A&A) process, are now able to “inherit” many of the security controls within the Access Control family as presented in NIST SP 800-53. In other words, if your agency is using an officially-sanctioned, accredited and authorized access control service, then the applications using this service will have an easier path to getting to and maintaining their own A&A. As new applications are developed for your enterprise, the access control portion can be “outsourced” to the EAM service, allowing your software engineers to focus on the mission instead of identity and access management development.



By having a central service where all the access requests and access responses are processed, access control events can now be logged in one location. Auditors will now be able to quickly answer the question of “Who accessed what and when?” This capability helps to satisfy NIST SP 800-53 security requirements outside of the Access Control family, such as the AU-2 Audit Events control family and associated control enhancements.

Now that logging and auditing have been enabled for externalized access control on your enterprise, this raw data can be pulled into your enterprise Security Information and Event Management (SIEM) tool(s) and used for enterprise monitoring, notably for triggers and alerts. For example, your agency’s security officers may want an alert in place should the authorization service send ten “DENY” access control responses in a row. This could be indicative of an attempt to gain access to unauthorized resources. Here another NIST SP 800-53 security control, SI-4 Information System Monitoring (SI), could be satisfied in part.

In summary, by migrating to an EAM service, your application development lifecycle, along with operations and maintenance, can be shortened, freeing up application developers to concentrate on the mission needs rather than access control. Digital policies can be constructed that reflect agency-wide security policies and uniformly applied throughout your enterprise to ensure that you know who is accessing what resources and when.

Axiomatics has taken the ABAC principles and extended them to applications, structured Databases and Big Data solutions. The cutting-edge innovative product suite enables agencies to audit and analyze policies to ensure compliance and mission needs. Call us to find out more.

11921 Freedom Drive Ste. 550
Two Fountain Square
Reston, VA 20190

federal@axiomatics.com
https://www.axiomatics.com/solutions/industry/federal-government