USE CASE

Security Compliance Using Externalized Authorization Central Decision Point for Fine-grained Access Control

AXIOMATICS
a LEONARDO company

Background

To effectively comply with various industry regulations, businesses require integrated, cost-effective information risk management solutions that can protect data and manage entitlements over applications. This document offers guidance on conducting an organizational IT risk assessment, and provides a template for determining what type of security controls are recommended to protect organizational operations and resources.

By using externalized authorization, developers can leverage a centrally managed authorization service instead of writing security rules into their code. This allows development teams to focus on functional aspects of the business and leave authorization rules to the business analysts or business process owners, saving time and money.

The specifics

WHAT

Enterprises can accelerate their authorization process by using dynamic, Attribute Based Access Control (ABAC).

WHY

Axiomatics is the leader in fine-grained, externalized dynamic authorization the most adaptable and scalable way to solve data security concerns. Today, leading automotive, pharmaceutical, energy, banking, and manufacturers use our solutions to safeguard and share sensitive data.

WHO

There are many internal stakeholders that benefit from a dynamic approach. ABAC helps assure CISOs with visibility and control over access to digital assets and that the policies developed are in accordance with the enterprise's IT security plan. Compliance officers and auditors also take an active interest in how ABAC helps 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

Enterprises that implement an externalized authorization 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 externalized authorization.

Applications are gateways to protected resources, such as sensitive health records, financial information, academic research, intellectual property, 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 with a policy-based approach can be applied uniformly to all the applications within an enterprise. This is achieved by transforming an enterprise’s natural language policies into digital policies, and then enforcing those policies through a centralized digital policy management store.

Ideally, users should be assigned permissions which represent a true reflection of current business policies and rules, risk mitigating precautions and context-related security measures.

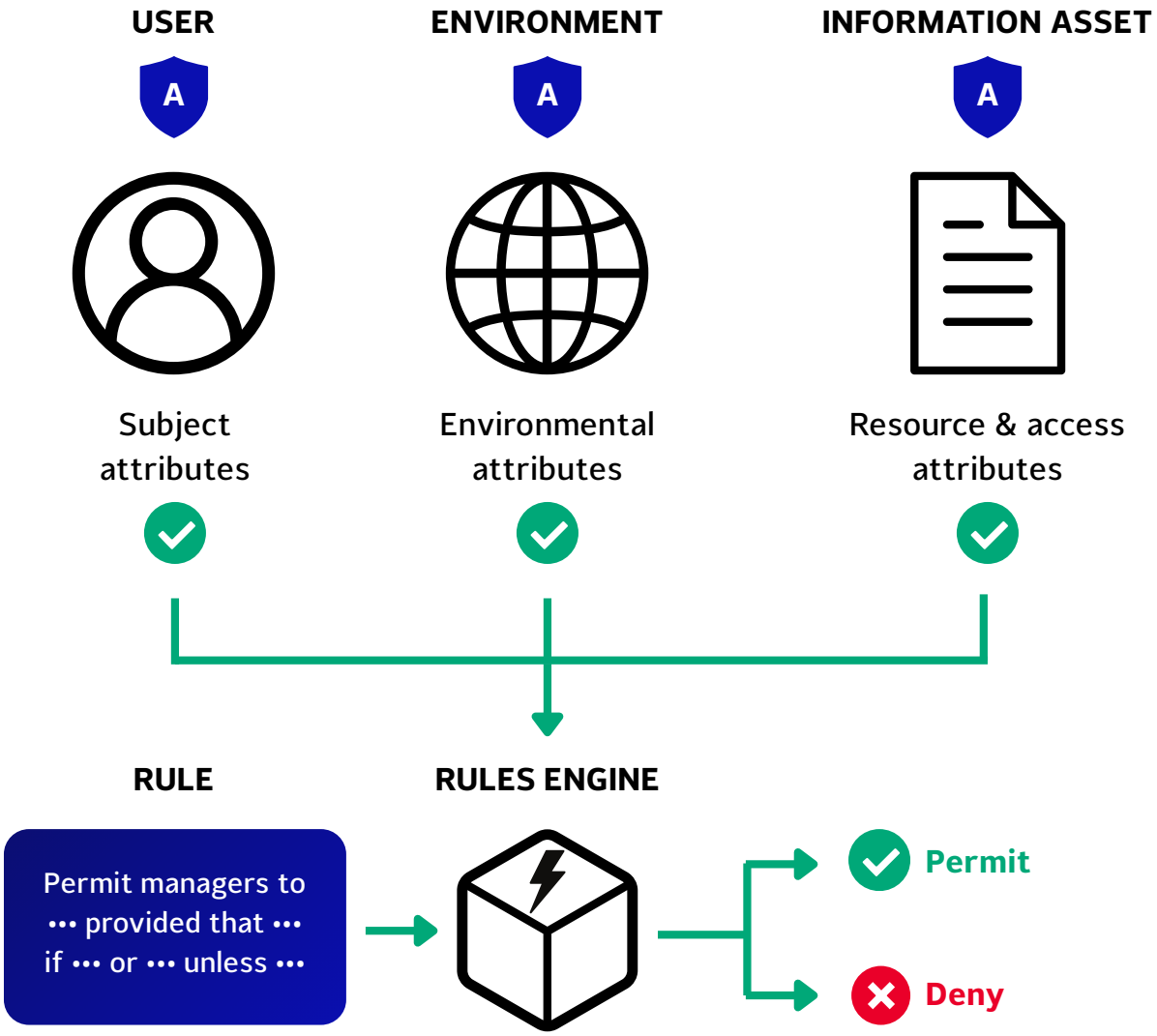
This is what the next generation entitlement management, Attribute Based Access Control (ABAC), delivers. ABAC implements business rules in context-aware and risk-mitigating policies. Rules combined in policies and policy sets become an exact definition rather than an approximation of authorizations based on business rules. They use attributes to describe when access should be permitted or denied. Attributes identify the user, the information asset, the action and the context in which access is being made.

The move from roles to rules thus allows the implementation of precise and finegrained authorization. This in turn also lays the foundation for dynamic and contextaware authorization. Rules are interpreted in real-time while considering context-related attributes such as risk indicators, time and location, user behavior patterns, the relation between the user and the information asset, etc.

Where RBAC provides coarse-grained, predefined and static access control configurations, ABAC offers finegrained rules which are evaluated dynamically in real-time.

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?”

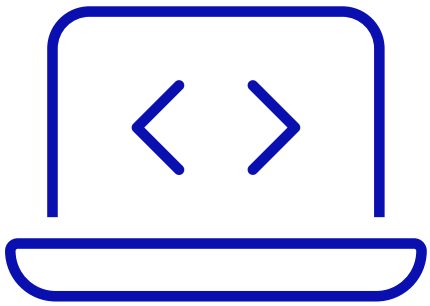
In summary, by migrating to dynamic authorization and ABAC, your application development lifecycle, along with operations and maintenance, can be shortened, freeing up application developers to concentrate on the mission needs rather than access control. Digital policies can be constructed that reflect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


USER
ENVIRONMENT
INFORMATION ASSET
A
A
A
Subject attributes
Environmental attributes
Resource & access attributes
RULE
RULES ENGINE
Permit managers to ••• provided that ••• if ••• or ••• unless •••
Permit
Deny

Take the next steps

Learn how how a security vendor can help secure your access control while allowing you to focus on your core business initiatives.

Meet with our solution experts for a demo of our Axiomatics Authorization Management Platform and discuss how our approach can save your organization time and money.



Stay connected and informed

Get the latest insights, announcements, and assets from our thought leaders and customer success team:

- Blog articles
- Press releases and announcements
- Resources, solution briefs, and tools
- Join us on LinkedIn
- Subscribe to our Linkedin Newsletter
- Subscribe to our YouTube channel

Axiomatics - a Leonardo Company is the originator and leading provider of runtime, fine-grained authorization delivered with attribute-based access control (ABAC) for applications, data, APIs, and microservices.

The company enables enterprises to effectively and efficiently connect Axiomatics' award-winning authorization platform to critical security implementations, such as Zero Trust or identity-first security. The world's largest enterprises and government agencies continually depend on Axiomatics' award-winning authorization platform to share sensitive, valuable, and regulated digital assets – but only to authorized users and in the right context.

Follow us on LinkedIn: https://linkedin.com/company/axiomatics

Join us on YouTube: https://youtube.com/@axiomatics

Learn more or request a demo of our solution:

axiomatics.com

info@axiomatics.com

US Office: +1 (312) 374-3443 | Europe Office: +46 8 51 510 240